Two p-adic L-functions and rational points on elliptic curves with supersingular reduction

Masato Kurihara and Robert Pollack

0 Introduction

Let E be an elliptic curve over $\mathbf{Q}$. We assume that E has good supersingular reduction at a prime p, and for simplicity, assume p is odd and $a_p = p + 1 - \#E(\mathbf{F}_p)$ is zero. Then, as the second author showed, the p-adic L-function $\mathcal{L}_{p,\alpha}(E)$ of E corresponding to $\alpha = \pm\sqrt{-p}$ (by Amice-Vélu and Vishik) can be written as

$$\mathcal{L}_{p,\alpha}(E) = f \log_p^+ + g \log_p^- \alpha$$

by using two Iwasawa functions f and $g \in \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$ ([20] Theorem 5.1). Here $\log_p^\pm$ is the $\pm$-log function and $\mathbf{Q}_\infty/\mathbf{Q}$ is the cyclotomic $\mathbf{Z}_p$-extension (precisely, see §1.3).

In Iwasawa theory for elliptic curves, the case when p is a supersingular prime is usually regarded to be more complicated than the ordinary case, but the fact that we have two nice Iwasawa functions f and g gives us some advantage in several cases. The aim of this paper is to give such examples.

0.1. Our first application is related to the weak Birch and Swinnerton-Dyer conjecture. Let $L(E, s)$ be the L-function of E. The so called weak Birch and Swinnerton-Dyer conjecture is the statement

Conjecture (Weak BSD)

$$L(E, 1) = 0 \Longleftrightarrow \mathrm{rank}\, E(\mathbf{Q}) > 0. \tag{1}$$

We know by Kolyvagin that the right hand side implies the left hand side, but the converse is still a very difficult conjecture. For a prime number p, let

$\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ be the Selmer group of E over $\mathbf{Q}$ with respect to the p-power torsion points $E[p^\infty]$. Hence $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ sits in an exact sequence

$$0 \longrightarrow E(\mathbf{Q}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}(E/\mathbf{Q})_{p^\infty} \longrightarrow Ш(E/\mathbf{Q})[p^\infty] \longrightarrow 0$$

where $Ш(E/\mathbf{Q})[p^\infty]$ is the p-primary component of the Tate-Shafarevich group of E over $\mathbf{Q}$. In this paper, we are interested in the following conjecture.

Conjecture 0.1

$$L(E,1) = 0 \Longleftrightarrow \#\,\mathrm{Sel}(E/\mathbf{Q})_{p^\infty} = \infty$$

This is equivalent to the weak Birch and Swinnerton-Dyer conjecture if we assume $\#Ш(E/\mathbf{Q})[p^\infty] < \infty$. (Of course, the problem is the implication from the left hand side to the right hand side.)

We note that Conjecture 0.1 is obtained as a corollary of the main conjecture in Iwasawa theory for E over the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$. We also remark that if the sign of the functional equation is -1, Conjecture 0.1 was proved by Skinner-Urban [24] and Nekovář [16] in the case when p is ordinary, and by Byoung-du Kim [10] in the case when p is supersingular.

In this paper, we will give a simple condition which can be checked numerically and which implies Conjecture 0.1.

Suppose that p is an *odd* supersingular prime with $a_p = 0$. We identify $\mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$ with $\mathbf{Z}_p[[T]]$ by the usual correspondence between a generator γ of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ and $1+T$. When we regard the above two Iwasawa functions f, g as elements in $\mathbf{Z}_p[[T]]$, we denote them by $f(T)$, $g(T)$. The interpolation property of $f(T)$ and $g(T)$ tells us that $f(0) = (p-1)L(E,1)/\Omega_E$ and $g(0) = 2L(E,1)/\Omega_E$ where Ω_E is the Néron period. Hence, if $L(E,1) \neq 0$, we have

$$\frac{f(T)}{g(T)}\Big|_{T=0} = \frac{p-1}{2}.$$

We conjecture that the converse is also true, namely

Conjecture 0.2

$$L(E,1) = 0 \Longleftrightarrow \frac{f(T)}{g(T)}\Big|_{T=0} \neq \frac{p-1}{2}$$

(Again, the problem is the implication from the left hand side to the right hand side.) Our first theorem says that Conjecture 0.2 implies Conjecture 0.1, namely

Theorem 0.3 *Assume that* $(f/g)(0)$ $\left(= \frac{f(T)}{g(T)}\Big|_{T=0}\right)$ *does not equal* $(p-1)/2$. *Then,* $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ *is infinite.*

This result in a different terminology was essentially obtained by Perrin-Riou (cf. [19] Proposition 4.10, see also §1.6 in this paper), but we will prove this theorem in §1.4 by a different and simple method, using a recent formulation of Iwasawa theory of an elliptic curve with supersingular reduction. In §1, we also review the recent formulation of such supersingular Iwasawa theory.

Conversely, assuming condition $(*)_0$ which will be introduced in §1.4 and which should always be true, we will show in §1.4 that the weak BSD conjecture (1) implies Conjecture 0.2, namely

Theorem 0.4 *Assume condition* $(*)_0$ *in* §1.4, *and* $\mathrm{rank}\, E(\mathbf{Q}) > 0$. *Then,* $(f/g)(0) \neq (p-1)/2$ *holds.*

Combining Theorems 0.3 and 0.4, we get

Corollary 0.5 *Assume* $(*)_0$ *in* §1.4 *and* $\#Ш(E/\mathbf{Q})[p^\infty] < \infty$. *Then, we have*

$$\mathrm{rank}\, E(\mathbf{Q}) > 0 \Longleftrightarrow \frac{f(T)}{g(T)}\Big|_{T=0} \neq \frac{p-1}{2}.$$

Note that the left hand side is algebraic information and the right hand side is p-adic analytic information. The weak BSD conjecture (1) is usually regarded to be a typical relation between algebraic and analytic information. The above Corollary 0.5 also gives such a relation, but in a different form. (Concerning the meaning of $(f/g)(0) \neq \frac{p-1}{2}$, see also §1.6.)

We note that $f(T)$ and $g(T)$ can be computed numerically and the condition $(f/g)(0) \neq (p-1)/2$ can be checked numerically. For example, for $N = 17$ and 32, we considered the quadratic twist $E = X_0(N)_d$ of the elliptic curve $X_0(N)$ by the Dirichlet character χ_d of conductor $d > 0$. For $p = 3$ (which is a supersingular prime in both cases with $a_p = 0$), we checked the condition $(f/g)(0) \neq (p-1)/2$ for all E_d such that $L(E_d, 1) = 0$ with $0 < d < 500$ and d prime to $3N$. We did this by computing $(f/g)(0) - (p-1)/2 \bmod 3^n$; the biggest n we needed was 7 for $E = X_0(32)_d$ with $d = 485$. For $N = 17$ and $d = 76, 104, 145, 157, 185, ...$ (resp. $N = 32$ and $d = 41, 65, 137, 145, 161, ...$) $\mathrm{ord}_T(f(T)) = \mathrm{ord}_T(g(T)) = 2$, so the corank of $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ should be 2. Our computation together with Theorem 0.3 implies that this corank is ≥ 1.

We give here one simple condition which implies $(f/g)(0) \neq (p-1)/2$. Put $r = \min\{\mathrm{ord}_T f(T), \mathrm{ord}_T g(T)\}$, and set $f^*(T) = T^{-r}f(T)$ and $g^*(T) = T^{-r}g(T)$. If $\mathrm{ord}_p(f^*(0)) \neq \mathrm{ord}_p(g^*(0))$, then $(f^*/g^*)(0)$ is not in $\mathbf{Z}_p^\times$ and hence cannot be $(p-1)/2$. Therefore, by Theorem 0.3 we have

Corollary 0.6 *If* $\mathrm{ord}_p(f^*(0)) \neq \mathrm{ord}_p(g^*(0))$, $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ *is infinite. In particular, if one of* $f^*(T)$ *or* $g^*(T)$ *has* λ*-invariant zero and the other has non-zero* λ*-invariant, then* $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ *is infinite.*

For example, we again consider $E = X_0(17)_d$ with $d > 0$ and $p = 3$. Then, the condition on the λ-invariants in Corollary 0.6 is satisfied by many examples, namely for $d = 29, 37, 40, 41, 44, 56, 65, ...$ with $r = 1$, and for $d = 145, 157, 185, 293, 409, ...$ with $r = 2$.

Corollary 0.6 implies a small result on the Main Conjecture (Proposition 1.5, see §1.5). The case $r = 1$ will be treated in detail in §2.

0.2. In 0.1, we explained that the computation of the value $(f/g)(0) - (p-1)/2$, or $f^{(r)}(0) - \frac{p-1}{2}g^{(r)}(0)$, yields information on the Selmer group $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ where $r = \min\{\mathrm{ord}_T f(T), \mathrm{ord}_T g(T)\}$. It is natural to ask what this value means. In the case $r = 1$, we can interpret this value very explicitly by using the p-adic Birch and Swinnerton-Dyer conjecture (cf. Bernardi and Perrin-Riou [1] and Colmez [4]).

In this case, for a generator P of $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}}$, the p-adic Birch and Swinnerton-Dyer conjecture predicts that $\log_{\hat{E}}(P)$ is related to $f'(0) - \frac{p-1}{2}g'(0)$ where $\log_{\hat{E}}$ is the logarithm of the formal group $\hat{E}$ (see §2.6 (11)). Using this formula for $\log_{\hat{E}}(P)$, we can find P numerically. More precisely, we compute

$$\exp_{\hat{E}}\left(\sqrt{-\frac{\left(f'(0) - \frac{p-1}{2}g'(0)\right) 2p\log(\kappa(\gamma))[\varphi(\omega_E), \omega_E]}{\mathrm{Tam}(E)}} \cdot \frac{\#E(\mathbf{Q})_{\mathrm{tors}}}{p+1}\right) \qquad (2)$$

which is a point on $E(\mathbf{Q}_p)$, and which would produce a point on $E(\mathbf{Q})$ with a slight modification (see §2.7). Namely, we can construct a rational point of infinite order p-adically in the case $r = 1$ as Rubin did in his paper [22] §3 for a CM elliptic curve.

Note here that we have an advantage in the supersingular case in that the two p-adic L-functions together encode $\log_{\hat{E}}(P)$ (and not just the p-adic height of a point).

We did the above computation for quadratic twists of the curve $X_0(17)$ with $p = 3$. We *found* a rational point on $X_0(17)_d$ *by this method* for *all* d

such that $0 < d < 250$ except for $d = 197$, $\gcd(d, 3 \cdot 17) = 1$, and the rank of $X_0(17)_d$ is 1. For example, for the curve

$$X_0(17)_{193} : y^2 + xy + y = x^3 - x^2 - 25609x - 99966422$$

we found the rational point

$$\left(\frac{915394662845247271}{25061097283236}, \frac{-878088421712236204458830141}{125458509476191439016}\right)$$

by this method, namely 3-adically. To get this rational point, we had to compute the value (2) modulo 3^{80} (to 80 3-adic digits) to recognize that the modified point constructed from the value (2) is a point on $E(\mathbf{Q})$. For the curve $X_0(32)$ and $p = 3$ we did a similar computation and found rational points on $X_0(32)_d$ for all d with $0 < d < 150$, $\gcd(d, 6)$, and the rank of $X_0(32)_d$ is 1. In §4, there are tables listing points for both of these curves.

To compute $f'(0)$ and $g'(0)$ to high accuracy, the usual definition of the p-adic L-function (namely, the computation of the Riemann sums to approximate $f'(0)$ and $g'(0)$) is not at all suitable. We use the theory of overconvergent modular symbols as in [21] and [6]. We will explain in detail in §2 this theory and the method to compute a rational point in practice.

0.3. Next, we study a certain important subgroup of the Selmer group over $\mathbf{Q}_\infty$. This is related to studying common divisors of $f(T)$ and $g(T)$. For any algebraic extension F of $\mathbf{Q}$, we define the fine Selmer group $\mathrm{Sel}_0(E/F)$ by

$$\mathrm{Sel}_0(E/F) = \mathrm{Ker}(\mathrm{Sel}(E/F)_{p^\infty} \longrightarrow \prod_{v|p} H^1(F_v, E[p^\infty]))$$

where $\mathrm{Sel}(E/F)_{p^\infty}$ is the Selmer group of E over F with respect to $E[p^\infty]$, and v ranges over primes of F lying over p. (The name "fine Selmer group" is due to J. Coates.) Our interest in this subsection is in $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)$.

Let $\mathbf{Q}_n$ be the intermediate field of $\mathbf{Q}_\infty/\mathbf{Q}$ with degree p^n. We put $e_0 = \mathrm{rank}\, E(\mathbf{Q})$ and $\Phi_0(T) = T$. For $n \geq 1$, we define

$$e_n = \frac{\mathrm{rank}\, E(\mathbf{Q}_n) - \mathrm{rank}\, E(\mathbf{Q}_{n-1})}{p^{n-1}(p-1)}$$

which is a non-negative integer, $\omega_n(T) = (1+T)^{p^n} - 1$, and $\Phi_n(T) = \omega_n(T)/\omega_{n-1}(T)$.

The Pontryagin dual $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee$ of the fine Selmer group over $\mathbf{Q}_\infty$ is a finitely generated torsion $\mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$-module by Kato [9]. Concerning the characteristic ideal, Greenberg raised the following problem (conjecture) (see §3.1)

Problem 0.7

$$\mathrm{char}(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = (\prod_{\substack{e_n \geq 1 \\ n \geq 0}} \Phi_n^{e_n - 1}).$$

We remark that this "conjecture" has the same flavor as his famous conjecture on the vanishing of the λ-invariants for class groups of totally real fields.

Let $\mathrm{Sel}^{\pm}(E/\mathbf{Q}_\infty)$ be Kobayashi's $\pm$-Selmer groups ([12], or see 1.5). By definition we have $\mathrm{Sel}_0(E/\mathbf{Q}_\infty) \subset \mathrm{Sel}^{\pm}(E/\mathbf{Q}_\infty)$. In this subsection, we assume the μ-invariant of $\mathrm{Sel}^{\pm}(E/\mathbf{Q}_\infty)$ vanishes. Using Kato's result [9] we know $g(T) \in \mathrm{char}\,\mathrm{Sel}^{+}(E/\mathbf{Q}_\infty)^\vee$, and $f(T) \in \mathrm{char}\,\mathrm{Sel}^{-}(E/\mathbf{Q}_\infty)^\vee$ (cf. Kobayashi [12] Theorem 1.3, see also 1.5). Hence, a generator of $\mathrm{char}\,\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee$ divides both $f(T)$ and $g(T)$. Thus, in the supersingular case, we can check this conjecture (Problem 0.7) numerically in many cases, by computing $f(T)$ and $g(T)$.

For example, suppose that $\mathrm{rank}\, E(\mathbf{Q}) = e_0$ and $\min\{\lambda(f(T)), \lambda(g(T))\} = e_0$. Then, we can show that the above "conjecture" is true and, moreover, $\mathrm{char}\,\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee = (T^{e_0'})$ where $e_0' = \max\{0, e_0 - 1\}$ (see Proposition 3.1). For $E = X_0(17)_d$ and $p = 3$, the condition of Proposition 3.1 is satisfied for all d such that $0 < d < 250$ except for $d = 104, 193, 233$. For these exceptional values, we also checked Problem 0.7 holds (see §3.3).

In §3.2 we raise a question on the greatest common divisor of $f(T)$ and $g(T)$ (Problem 3.2), and study a relation with the above Greenberg "conjecture" (see Propositions 3.3 and 3.4).

We would like to heartily thank R. Greenberg for fruitful discussions on all subjects in this paper, and for his hospitality when both of us were invited to the University of Washington in May 2004. Furthermore, we learned to use Wingberg's result from him when we studied the problem in Proposition 3.4 (1). We would also like to express our hearty thanks to G. Stevens for his helpful suggestion when we studied the example (the case $d = 193$) in §3.3.

1 Iwasawa theory of an elliptic curve with supersingular reduction

1.1. $\pm$-Coleman homomorphisms. Kobayashi defined in [12] §8 $\pm$-Coleman homomorphisms. We will give here a slightly different construction of these homomorphisms using the results of the first author in [13].

Suppose that E has good supersingular reduction at an odd prime p with $a_p = p + 1 - \#E(\mathbf{F}_p) = 0$. We denote by $T = T_p(E)$ the Tate module, and set $V = T \otimes \mathbf{Q}_p$. For $n \geq 0$, let $\mathbf{Q}_{p,n}$ denote the intermediate field of the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_{p,\infty}/\mathbf{Q}_p$ of the p-adic field $\mathbf{Q}_p$ such that $[\mathbf{Q}_{p,n} : \mathbf{Q}_p] = p^n$. We set $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]] = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_{p,\infty}/\mathbf{Q}_p)]]$, and identify Λ with $\mathbf{Z}_p[[T]]$ by identifying γ with $1 + T$. We put

$$\mathbf{H}^1_{\mathrm{loc}} = \varprojlim H^1(\mathbf{Q}_{p,n}, T)$$

where the limit is taken with respect to the corestriction maps. We will define two Λ-homomorphisms

$$\mathrm{Col}^{\pm} : \mathbf{H}^1_{\mathrm{loc}} \longrightarrow \Lambda.$$

Let $D = D_{dR}(V)$ be the Dieudonné module which is a two dimensional $\mathbf{Q}_p$-vector space. Let ω_E be the Néron differential which we regard as an element of D. Since D is isomorphic to the crystalline cohomology $H^1_{cris}(E \bmod p/\mathbf{Q}_p)$, the Frobenius operator φ acts on D and satisfies $\varphi^{-2} - a_p\varphi^{-1} + p = \varphi^{-2} + p = 0$.

We take a generator (ζ_{p^n}) of $\mathbf{Z}_p(1)$; namely, ζ_{p^n} is a primitive p^n-th root of unity, and $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for any $n \geq 1$. For $n \geq 1$ and $x \in D$, put

$$\gamma_n(x) = \sum_{i=0}^{n-1} \varphi^{i-n}(x) \otimes \zeta_{p^{n-i}} + (1-\varphi)^{-1}(x) \in D \otimes \mathbf{Q}_p(\mu_{p^n}).$$

Putting $\mathcal{G}_{n+1} = \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^{n+1}})/\mathbf{Q}_p)$, we define

$$P_n : H^1(\mathbf{Q}_p(\mu_{p^{n+1}}), T) \longrightarrow \mathbf{Q}_p[\mathcal{G}_{n+1}]$$

by

$$P_n(z) = \frac{1}{[\varphi(\omega_E), \omega_E]} \sum_{\sigma \in \mathcal{G}_{n+1}} \mathrm{Tr}_{\mathbf{Q}_p(\mu_{p^{n+1}})/\mathbf{Q}_p}([\gamma_{n+1}(\varphi^{n+2}(\omega_E))^\sigma, \exp^*(z)])\sigma.$$

Here

$$\exp^* : H^1(\mathbf{Q}_p(\mu_{p^{n+1}}), T) \longrightarrow D \otimes \mathbf{Q}_p(\mu_{p^{n+1}})$$

is the dual exponential map of Bloch and Kato (which is the dual of the exponential map: $D \otimes \mathbf{Q}_p(\mu_{p^{n+1}}) \longrightarrow H^1(\mathbf{Q}_p(\mu_{p^{n+1}}), T)$), and $[x, y] \in D \otimes \mathbf{Q}_p(\mu_{p^{n+1}})$ is the cup product of the de Rham cohomology for x, $y \in D \otimes \mathbf{Q}_p(\mu_{p^{n+1}})$. In this, $[\varphi(\omega_E), \omega_E] \in \mathbf{Z}_p$ plays the role of a p-adic period. By Proposition 3.6 in [13], we have

$$P_n(z) \in \mathbf{Z}_p[\mathcal{G}_{n+1}]$$

(note that we slightly changed the notation γ_n, P_n from [13]).

Put $G_n = \mathrm{Gal}(\mathbf{Q}_{p,n}/\mathbf{Q}_p)$, and let $i : H^1(\mathbf{Q}_{p,n}, T) \longrightarrow H^1(\mathbf{Q}_p(\mu_{p^{n+1}}), T)$ and $\pi : \mathbf{Z}_p[\mathcal{G}_{n+1}] \longrightarrow \mathbf{Z}_p[G_n]$ be the natural maps. We define

$$\mathcal{P}_n : H^1(\mathbf{Q}_{p,n}, T) \longrightarrow \mathbf{Z}_p[G_n]$$

by

$$\mathcal{P}_n(z) = \frac{1}{p-1} \pi \circ P_n(i(z)).$$

These elements satisfy a distribution property; namely, we have

$$\pi_{n,n-1} \mathcal{P}_n(z) = -\nu_{n-2,n-1} \mathcal{P}_{n-2}(N_{n,n-2}(z))$$

where $\pi_{n,n-1} : \mathbf{Z}_p[G_n] \longrightarrow \mathbf{Z}_p[G_{n-1}]$ is the natural projection, $\nu_{n-2,n-1} : \mathbf{Z}_p[G_{n-2}] \longrightarrow \mathbf{Z}_p[G_{n-1}]$ is the norm map such that $\sigma \mapsto \Sigma\tau$ (for $\sigma \in G_{n-2}$, τ ranges over elements in G_{n-1} such that $\pi_{n-1,n-2}(\tau) = \sigma$), and $N_{n,n-2} : H^1(\mathbf{Q}_{p,n}, T) \longrightarrow H^1(\mathbf{Q}_{p,n-2}, T)$ is the corestriction map. This relation can be proved by showing $\psi(\pi_{n,n-1}\mathcal{P}_n(z)) = \psi(-\nu_{n-2,n-1}\mathcal{P}_{n-2}(N_{n,n-2}(z)))$ for any character ψ of G_{n-1} (cf. the proof of Lemma 7.2 in [13]).

Our identification of γ with $1+T$, gives an identification of $\mathbf{Z}_p[G_n]$ with $\mathbf{Z}_p[T]/((1+T)^{p^n} - 1)$. Set $\omega_m = (1+T)^{p^m} - 1$, and $\Phi_m = \omega_m/\omega_{m-1}$ which is the p^m-th cyclotomic polynomial evaluated at $1+T$. The above distribution relation implies that Φ_{n-1} divides $\mathcal{P}_n(z)$. By induction on n, we can show that $\Phi_{n-1}\Phi_{n-3}\cdot\ldots\cdot\Phi_1$ divides $\mathcal{P}_n(z)$ if n is even, and $\Phi_{n-1}\Phi_{n-3}\cdot\ldots\cdot\Phi_2$ divides $\mathcal{P}_n(z)$ if n is odd. Put

$$\omega_n^+ = \prod_{2 \le m \le n, 2|m} \Phi_m, \quad \omega_n^- = \prod_{1 \le m \le n, 2\nmid m} \Phi_m.$$

Suppose that z is an element in $\mathbf{H}^1_{\mathrm{loc}}$, and $z_n \in H^1(\mathbf{Q}_{p,n}, T)$ is its image. Suppose at first n is odd, and write $\mathcal{P}_n(z_n) = \omega_n^+ h_n(T)$ with $h_n(T) \in \mathbf{Z}_p[T]/(\omega_n)$. Then, $h_n(T)$ is uniquely determined in $\mathbf{Z}_p[T]/(T\omega_n^-)$ because $\omega_n^+\omega_n^- T = \omega_n$; so we regard $h_n(T)$ as an element in this ring. By the above distribution property, we know that $((-1)^{(n+1)/2} h_n(T))_{n:\mathrm{odd} \ge 1}$ is a projective

system with respect to the natural maps $\mathbf{Z}_p[T]/(T\omega_{n+2}^-) \longrightarrow \mathbf{Z}_p[T]/(T\omega_n^-)$. Hence, it defines an element $h(T) \in \varprojlim \mathbf{Z}_p[T]/(T\omega_n^-) = \mathbf{Z}_p[[T]] = \Lambda$. We define $\mathrm{Col}^+(z) = h(T)$.

Next, suppose n is even. We write $\mathcal{P}_n(z_n) = \omega_n^- k_n(T)$ with $k_n(T) \in \mathbf{Z}_p[T]/(T\omega_n^+)$. By the same method as above, the distribution property implies that $((-1)^{(n+2)/2}k_n(T))_{n:\mathrm{even}\geq 1}$ is a projective system, so it defines $k(T) \in \varprojlim \mathbf{Z}_p[T]/(T\omega_n^+) = \mathbf{Z}_p[[T]] = \Lambda$. We define $\mathrm{Col}^-(z) = k(T)$. Thus, we have obtained two power series from $z \in \mathbf{H}^1_{\mathrm{loc}}$. We define $\mathrm{Col} : \mathbf{H}^1_{\mathrm{loc}} \longrightarrow \Lambda \oplus \Lambda$ by $\mathrm{Col}(z) = (\mathrm{Col}^+(z), \mathrm{Col}^-(z)) = (h(T), k(T))$.

The next lemma will be useful in what follows.

Lemma 1.1 *Suppose* $z \in \mathbf{H}^1_{\mathrm{loc}}$, $\mathrm{Col}^+(z) = h(T)$, *and* $\mathrm{Col}^-(z) = k(T)$. *Then,*

$$h(0) = \frac{p(p-1)}{p+1}\frac{\exp^*(z_0)}{\omega_E} \quad \textit{and} \quad k(0) = \frac{2p}{p+1}\frac{\exp^*(z_0)}{\omega_E}$$

where z_0 *is the image of* z *in* $H^1(\mathbf{Q}_p, T)$, *and* $\exp^*(z_0)/\omega_E$ *is the element* $a \in \mathbf{Q}_p$ *such that* $\exp^*(z_0) = a\omega_E$.

We note that $\exp^*(z_0)/\omega_E$ is known to be in $p^{-1}\mathbf{Z}_p$ (cf. [23] Proposition 5.2), hence the right hand side of the above formula is in $\mathbf{Z}_p$.

Proof. This follows from the construction of $\mathrm{Col}^{\pm}(z)$ and Lemma 3.5 in [13] (cf. the proof of Lemma 7.2 in [13], pg. 220).

1.2. An exact sequence. We have defined

$$\mathrm{Col} = \mathrm{Col}^+ \oplus \mathrm{Col}^- : \mathbf{H}^1_{\mathrm{loc}} \longrightarrow \Lambda \oplus \Lambda.$$

This homomorphism induces

Proposition 1.2 *We have an exact sequence*

$$0 \longrightarrow \mathbf{H}^1_{\mathrm{loc}} \xrightarrow{\mathrm{Col}} \Lambda \oplus \Lambda \xrightarrow{\rho} \mathbf{Z}_p \longrightarrow 0$$

where ρ *is the map defined by* $\rho(h(T), k(T)) = h(0) - \frac{p-1}{2}k(0)$.

Proof. First of all, we note that $\mathbf{H}^1_{\mathrm{loc}}$ is a free Λ-module of rank 2. In fact, since $H^0(\mathbf{Q}_{p,\infty}, E[p]) = 0$, it follows that $H^1(\mathbf{Q}_p, E[p^\infty]) \xrightarrow{\simeq} H^1(\mathbf{Q}_{p,\infty}, E[p^\infty])^{\mathrm{Gal}(\mathbf{Q}_{p,\infty}/\mathbf{Q}_p)}$ is bijective. Taking the dual, we get an isomorphism $(\mathbf{H}^1_{\mathrm{loc}})_{\mathrm{Gal}(\mathbf{Q}_{p,\infty}/\mathbf{Q}_p)} \simeq H^1(\mathbf{Q}_p, T)$. Since $H^0(\mathbf{Q}_p, E[p]) = H^2(\mathbf{Q}_p, E[p]) = 0$, $H^1(\mathbf{Q}_p, T)$ is a free $\mathbf{Z}_p$-module of rank 2, and so $\mathbf{H}^1_{\mathrm{loc}}$ is a free Λ-module of rank 2.

By Lemma 1.1, we know $\rho \circ \mathrm{Col} = 0$. Hence, to prove Proposition 1.2, it suffices to show that the cokernel of Col is isomorphic to $\mathbf{Z}_p$.

Kobayashi defined two subgroups $E^{\pm}(\mathbf{Q}_{p,n})$ of $E(\mathbf{Q}_{p,n}) \otimes \mathbf{Z}_p$ ([12] Definition 8.16). We will explain these subgroups in a slightly different way (this idea is due to R. Greenberg). Since $E(\mathbf{Q}_{p,n}) \otimes \mathbf{Q}_p$ is the regular representation of G_n, it decomposes into $\bigoplus_{i=0}^{n} V_i$ where the V_i's are irreducible representations such that $\dim_{\mathbf{Q}_p} V_0 = 1$, and $\dim_{\mathbf{Q}_p} V_i = p^{i-1}(p-1)$ for $i > 0$. Then $E^{+}(\mathbf{Q}_{p,n})$ (resp. $E^{-}(\mathbf{Q}_{p,n})$) is defined to be the subgroup consisting of all points $P \in E(\mathbf{Q}_{p,n}) \otimes \mathbf{Z}_p$ such that the image of P in V_i is zero for every odd i (resp. for every positive even i). We define $E^{\pm}(\mathbf{Q}_{p,\infty})$ as the direct limit of $E^{\pm}(\mathbf{Q}_{p,n})$. By definition, the sequence

$$\begin{aligned} 0 \longrightarrow E(\mathbf{Q}_p) \otimes \mathbf{Q}_p/\mathbf{Z}_p \quad &\longrightarrow \quad E^{+}(\mathbf{Q}_{p,\infty}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \oplus E^{-}(\mathbf{Q}_{p,\infty}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \\ &\longrightarrow \quad E(\mathbf{Q}_{p,\infty}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow 0 \end{aligned}$$

is exact. Since p is supersingular, $E(\mathbf{Q}_{p,\infty}) \otimes \mathbf{Q}_p/\mathbf{Z}_p = H^1(\mathbf{Q}_{p,\infty}, E[p^{\infty}])$. We also know that $E^{\pm}(\mathbf{Q}_{p,\infty}) \otimes \mathbf{Q}_p/\mathbf{Z}_p$ is the exact annihilator of the kernel of $\mathrm{Col}^{\pm}$ with respect to the cup product ([12] Proposition 8.18). Hence, taking the dual of the above exact sequence, we get $\mathrm{Coker}(\mathrm{Col}) \simeq (E(\mathbf{Q}_p) \otimes \mathbf{Q}_p/\mathbf{Z}_p)^{\vee} \simeq \mathbf{Z}_p$, which completes the proof.

1.3. p-adic L-functions and Kato's zeta elements. We now consider global cohomology groups. For $n \geq 0$, let $\mathbf{Q}_n$ denote the intermediate field of $\mathbf{Q}_{\infty}/\mathbf{Q}$ with degree p^n. We define

$$\mathbf{H}^1_{\mathrm{glob}} = \varprojlim H^1(\mathbf{Q}_n, T) = \varprojlim H^1_{et}(O_{\mathbf{Q}_n}[1/S], T)$$

where the limit is taken with respect to the corestriction maps, and S is the product of the primes of bad reduction and p. The image of $z \in \mathbf{H}^1_{\mathrm{glob}}$ in $\mathbf{H}^1_{\mathrm{loc}}$ we continue to denote by z. In our situation, $\mathbf{H}^1_{\mathrm{glob}}$ was proved to be a free Λ-module of rank 1 (Kato [9] Theorem 12.4). Kato constructed an element $z_K = ((z_K)_n)_{n \geq 0} \in \mathbf{H}^1_{\mathrm{glob}}$ with the following properties [9]. For a faithful character ψ of $G_n = \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$ with $n > 0$,

$$\sum_{\sigma \in G_n} \psi(\sigma) \exp^*(\sigma(z_K)_n) = \omega_E \frac{L(E, \psi, 1)}{\Omega_E},$$

and

$$\exp^*((z_K)_0) = \omega_E (1 - a_p p^{-1} + p^{-1}) \frac{L(E, 1)}{\Omega_E}$$

where $\exp^* : H^1(\mathbf{Q}_{p,n}, T) \longrightarrow D \otimes \mathbf{Q}_{p,n}$ is the dual exponential map.

Suppose that $\theta_{\mathbf{Q}_n} \in \mathbf{Z}_p[G_n]$ is the modular element of Mazur and Tate [15], which satisfies the distribution property $\pi_{n,n-1}\theta_{\mathbf{Q}_n} = -\nu_{n-2,n-1}\theta_{\mathbf{Q}_{n-2}}$, and the property that for a faithful character ψ of $G_n = \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$ with $n > 0$,

$$\psi(\theta_{\mathbf{Q}_n}) = \tau(\psi)\frac{L(E,\psi^{-1},1)}{\Omega_E}$$

where $\tau(\psi)$ is the Gauss sum, and $\psi : \mathbf{Z}_p[G_n] \longrightarrow \mathbf{Z}_p[\mathrm{Image}\,\psi]$ is the ring homomorphism induced by ψ.

Let α and β be two roots of $t^2 + p = 0$. We have two p-adic L-functions $\mathcal{L}_{p,\alpha}$ and $\mathcal{L}_{p,\beta}$ by Amice-Vélu and Vishik, which are in $\mathcal{H}_\infty \otimes \mathbf{Q}_p(\sqrt{-p})$ where

$$\mathcal{H}_\infty = \left\{ \sum_{n=0}^{\infty} a_n T^n \in \mathbf{Q}_p[[T]]; \lim_{n\to\infty} |a_n|_p n^{-h} = 0 \text{ for some } h \in \mathbf{Z}_{>0} \right\}.$$

As the second author proved in [20], there are two Iwasawa functions $f(T)$ and $g(T)$ in $\mathbf{Z}_p[[T]]$ such that

$$\mathcal{L}_{p,\alpha}(T) = f(T)\log^+(T) + \alpha g(T)\log^-(T) \tag{3}$$

and

$$\mathcal{L}_{p,\beta}(T) = f(T)\log^+(T) + \beta g(T)\log^-(T) \tag{4}$$

where $\log^+(T) = p^{-1}\Pi_{n>0}\frac{1}{p}\Phi_{2n}(T)$ and $\log^-(T) = p^{-1}\Pi_{n>0}\frac{1}{p}\Phi_{2n-1}(T)$.

Let $\mathcal{P}_n$ be as in §1.1, and $z_K = ((z_K)_n)$ be the zeta element of Kato. By Lemma 7.2 in [13] by the first author, we have

$$\mathcal{P}_n((z_K)_n) = \theta_{\mathbf{Q}_n} \tag{5}$$

(we note that we need no assumption (for example on $L(E,1)$) to get (5)). Since we know that $\mathcal{L}_{p,\alpha}$ is also obtained as the limit of

$$\alpha^{-n-1}(\theta_{\mathbf{Q}_n} - \alpha^{-1}\nu_{n-1,n}\theta_{\mathbf{Q}_{n-1}}),$$

using (5), we obtain

$$\mathcal{L}_{p,\alpha}(T) = \mathrm{Col}^+(z_K)\log^+(T) + \alpha\,\mathrm{Col}^-(z_K)\log^-(T).$$

Comparing this formula with (3), we have proved

Theorem 1.3 (**Kobayashi [12] Theorem 6.3**) *Let z_K be Kato's zeta element, and f, g be the Iwasawa functions as in* (3). *Then, we have* $\mathrm{Col}^+(z_K) = f(T)$ *and* $\mathrm{Col}^-(z_K) = g(T)$.

1.4. Proofs of Theorems 0.3 and 0.4. We begin by proving Theorem 0.3. For a non-zero element z in $\mathbf{H}^1_{\mathrm{glob}}$, we write $\mathrm{Col}(z) = (h_z(T), k_z(T))$. Since $\mathbf{H}^1_{\mathrm{glob}}$ is free of rank 1 over Λ ([9] Theorem 12.4), $h_z(T)/k_z(T)$ does not depend on the choice of $z \in \mathbf{H}^1_{\mathrm{glob}}$. So choosing $z = z_K$, we have by Theorem 1.3, that $h_z(T)/k_z(T) = f(T)/g(T)$ for all non-zero $z \in \mathbf{H}^1_{\mathrm{glob}}$.

Let ξ be a generator of $\mathbf{H}^1_{\mathrm{glob}}$. Suppose that $h_\xi(0) \neq 0$. By Proposition 1.2, $\rho(\mathrm{Col}(\xi)) = 0$, so we get $k_\xi(0) \neq 0$ and $h_\xi(0)/k_\xi(0) = (f/g)(0) = (p-1)/2$. This contradicts our assumption. Hence, $h_\xi(0) = 0$. This implies that the image $\xi_{\mathbf{Q}_p}$ of ξ in $H^1(\mathbf{Q}_p, T)$ satisfies $\exp^*(\xi_{\mathbf{Q}_p}) = 0$ by Lemma 1.1, so $\xi_{\mathbf{Q}_p}$ is in $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$. Hence, the image $\xi_{\mathbf{Q}}$ of ξ in $H^1(\mathbf{Q}, T)$ is in $\mathrm{Sel}(E/\mathbf{Q}, T)$ which is the Selmer group of $E/\mathbf{Q}$ with respect to T. Since $\mathbf{H}^1_{\mathrm{glob}} = H^1(\mathbf{Q}, \Lambda \otimes T)$, from an exact sequence $0 \longrightarrow \Lambda \otimes T \longrightarrow \Lambda \otimes T \longrightarrow T \longrightarrow 0$, the natural map $(\mathbf{H}^1_{\mathrm{glob}})_{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})} \longrightarrow H^1(\mathbf{Q}, T)$ is injective ($(\mathbf{H}^1_{\mathrm{glob}})_{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})}$ is the $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$-coinvariants of $\mathbf{H}^1_{\mathrm{glob}}$). Thus, $\xi_{\mathbf{Q}} \in \mathrm{Sel}(E/\mathbf{Q}, T)$ is of infinite order. Therefore, $\#\,\mathrm{Sel}(E/\mathbf{Q}, T) = \infty$, which implies $\#\,\mathrm{Sel}(E/\mathbf{Q})_{p^\infty} = \infty$ and establishes Theorem 0.3.

Next, we introduce condition $(*)_0$. We consider the composite $\mathbf{H}^1_{\mathrm{glob}} \longrightarrow H^1(\mathbf{Q}, T) \longrightarrow H^1(\mathbf{Q}_p, T)$ of natural maps, and the property

$(*)_0$ $\qquad\qquad \mathbf{H}^1_{\mathrm{glob}} \longrightarrow H^1(\mathbf{Q}_p, T)$ is not the zero map.

This property $(*)_0$ should always be true. In fact, it is a consequence of the p-adic Birch and Swinnerton-Dyer conjecture. More precisely, it follows from a conjecture that a certain p-adic height pairing is non-degenerate (see Perrin-Riou [17] pg. 979 Conjecture 3.3.7 B and Remarque iii)).

We now prove Theorem 0.4. As we saw in the proof of Proposition 1.2, $\mathbf{H}^1_{\mathrm{loc}}$ is a free Λ-module of rank 2. The p-adic rational points $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$ is a direct summand of $H^1(\mathbf{Q}_p, T)$; hence, we can take a basis e_1, e_2 of $\mathbf{H}^1_{\mathrm{loc}}$ such that the image e_1^0 of e_1 in $H^1(\mathbf{Q}_p, T)$ is not in $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$, and the image e_2^0 of e_2 in $H^1(\mathbf{Q}_p, T)$ generates $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$. Since e_1^0 is not in $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$, $\exp^*(e_1^0) \neq 0$, and, by Lemma 1.1, $\mathrm{Col}^+(e_1)(0) \neq 0$, and $\mathrm{Col}^-(e_1)(0) \neq 0$. Since e_2^0 is in $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$, by Lemma 1.1, $\mathrm{Col}^+(e_2)(0) = \mathrm{Col}^-(e_2)(0) = 0$. We also have that $\mathrm{Col}^+(e_2)'(0) \neq 0$ and $\mathrm{Col}^-(e_2)'(0) \neq 0$. This follows from the fact that the determinant of the Λ-homomorphism $\mathrm{Col} : \mathbf{H}^1_{\mathrm{loc}} \longrightarrow \Lambda \oplus \Lambda$ is T modulo units by Proposition 1.2. We also note that $\mathrm{Col}^+(e_2)'(0) - \frac{p-1}{2}\mathrm{Col}^-(e_2)'(0) \neq 0$. Indeed, since $(\mathrm{Col}^+(e_1)/\mathrm{Col}^-(e_1))(0) = (p-1)/2$, if we had $(\mathrm{Col}^+(e_2)/\mathrm{Col}^-(e_2))(0) = (p-1)/2$, we would have

$$\mathrm{Image}(\mathrm{Col}) \cap T(\Lambda \oplus \Lambda) \subset ((p-1)/2, 1)T\Lambda + T^2(\Lambda \oplus \Lambda),$$

which contradicts Proposition 1.2.

Now we assume $(*)_0$ and $\operatorname{rank} E(\mathbf{Q}) > 0$. Let ξ, $h_\xi(T)$, $k_\xi(T)$, ... be as in the proof of Theorem 0.3. We write $\xi = a(T)e_1 + b(T)e_2$ with $a(T)$, $b(T) \in \Lambda$. Since $\operatorname{rank} E(\mathbf{Q}) > 0$, $E(\mathbf{Q}) \otimes \mathbf{Q}_p \longrightarrow E(\mathbf{Q}_p) \otimes \mathbf{Q}_p$ is surjective. So the image of $H^1(\mathbf{Q}, T) \longrightarrow H^1(\mathbf{Q}_p, T)$ is in $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$ by Lemma 1.4 below which we will prove later. Therefore, $a(0) = 0$. Hence, $(*)_0$ implies that $b(0) \neq 0$. Thus, we get

$$h'_\xi(0) - \frac{p-1}{2} k'_\xi(0) = b(0) \left(\operatorname{Col}^+(e_2)'(0) - \frac{p-1}{2} \operatorname{Col}^-(e_2)'(0) \right) \neq 0.$$

Hence,

$$\frac{f(T)}{g(T)}\Big|_{T=0} = \frac{h'_\xi(0)}{k'_\xi(0)} \neq \frac{p-1}{2},$$

which completes the proof.

Our last task in this subsection is to prove the following well-known property.

Lemma 1.4 . *Let $V = T \otimes \mathbf{Q}$. The image of $H^1(\mathbf{Q}, V) \longrightarrow H^1(\mathbf{Q}_p, V)$ is a one dimensional $\mathbf{Q}_p$-vector space.*

Proof of Lemma 1.4. We first note that $H^1(\mathbf{Q}, V) = H^1(\mathbf{Z}[1/S], V)$ where S is the product of the primes of bad reduction and p. Since V is self-dual, by the Tate-Poitou duality we have an exact sequence

$$H^1(\mathbf{Q}, V) \xrightarrow{i} H^1(\mathbf{Q}_p, V) \xrightarrow{i^\vee} H^1(\mathbf{Q}, V)^\vee$$

where $i^\vee : H^1(\mathbf{Q}_p, V) = H^1(\mathbf{Q}_p, V)^\vee \longrightarrow H^1(\mathbf{Q}, V)^\vee$ is obtained as the dual of $i : H^1(\mathbf{Q}, V) \longrightarrow H^1(\mathbf{Q}_p, V)$. This shows that $\dim \operatorname{Image}(i) = \dim \operatorname{Image}(i^\vee) = \dim \operatorname{Coker}(i)$. Thus, we obtain $\dim \operatorname{Image}(i) = 1$ from $\dim H^1(\mathbf{Q}_p, V) = 2$.

1.5. Main Conjecture. We review the main conjectures in our case. We define $\operatorname{Sel}^\pm(E/\mathbf{Q}_\infty)$ to be the Selmer group which is defined by replacing the local condition at p with $E^\pm(\mathbf{Q}_{p,\infty}) \otimes \mathbf{Q}_p/\mathbf{Z}_p$ (see the proof of Proposition 1.2). Then, the main conjecture is formulated as

$$\operatorname{char} \operatorname{Sel}^+(E/\mathbf{Q}_\infty)^\vee = (g(T))$$

and

$$\operatorname{char} \operatorname{Sel}^-(E/\mathbf{Q}_\infty)^\vee = (f(T))$$

where $(*)^\vee$ is the Pontryagin dual (Kobayashi [12]). These two conjectures are equivalent to each other ([12] Theorem 7.4) and, furthermore, each of them is equivalent to

$$\operatorname{char} \mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee = \operatorname{char}(\mathbf{H}^1_{\mathrm{glob}}/ < z_K >)$$

where $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)$ is defined as in 0.3. The inclusion $\supset$ is proved by using Kato's result [9] up to μ-invariants (Kobayashi [12] Theorem 1.3).

We give here a corollary of Corollary 0.6 in §0.1.

Proposition 1.5 *Assume that* $L(E,1) = 0$, $\mu(f(T)) = \mu(g(T)) = 0$, *and*

$$1 = \min\{\lambda(f(T)), \lambda(g(T))\} < \max\{\lambda(f(T)), \lambda(g(T))\}.$$

Then, the Iwasawa main conjecture for E *is true; namely,* $\operatorname{char} \mathrm{Sel}^+(E/\mathbf{Q}_\infty)^\vee = (g(T))$ *and* $\operatorname{char} \mathrm{Sel}^-(E/\mathbf{Q}_\infty)^\vee = (f(T))$.

Proof. Corollary 0.6 implies that $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ is infinite. Hence, by the control theorem for $\mathrm{Sel}^\pm(E/\mathbf{Q}_\infty)$ ([12] Theorem 9.3), T divides the characteristic power series of $\mathrm{Sel}^\pm(E/\mathbf{Q}_\infty)^\vee$, and thus, T divides $f(T)$ and $g(T)$. Then, by our assumption, one of $(f(T))$ or $(g(T))$ equals (T). Hence, the main conjecture for one of $\mathrm{Sel}^+(E/\mathbf{Q}_\infty)$ or $\mathrm{Sel}^-(E/\mathbf{Q}_\infty)$ holds. This implies that both statements are true ([12] Theorem 7.4).

As an example, we consider the quadratic twist $E = X_0(17)_d$ as in §0.1. Then, the condition in Proposition 1.5 is satisfied by $X_0(17)_d$ for $d = 29, 37, 40, 41, 44, 56, 65, \ldots$. For example, when $d = 37$, we have

$$\operatorname{char} \mathrm{Sel}^+(E/\mathbf{Q}_\infty)^\vee = (T) \text{ and } \operatorname{char} \mathrm{Sel}^-(E/\mathbf{Q}_\infty)^\vee = ((1+T)^3 - 1).$$

Hence, if we assume the finiteness of $Ш(E/\mathbf{Q}(\cos 2\pi/9))[3^\infty]$, we know that $\operatorname{rank} E(\mathbf{Q}) = 1$ and $\operatorname{rank} E(\mathbf{Q}(\cos 2\pi/9)) = 3$. Note that we get this conclusion just from analytic information (the computation of modular symbols).

1.6. Remark. We consider in this subsection a more general case. We assume that E has good reduction at an odd prime p. If p is ordinary, we assume that E does not have complex multiplication. Let α, β be the two roots of $x^2 - a_p x + p = 0$ in an algebraic closure of $\mathbf{Q}_p$ where $a_p = p + 1 - \#E(\mathbf{F}_p)$. If p is ordinary, we take α to be a unit in $\mathbf{Z}_p$ as usual. If p is a supersingular prime, we have two p-adic L-functions $\mathcal{L}_{p,\alpha}$ and $\mathcal{L}_{p,\beta}$ by Amice-Vélu and Vishik.

If p is ordinary, $\mathcal{L}_{p,\alpha}$ is the p-adic L-function by Mazur and Swinnerton-Dyer. The other function $\mathcal{L}_{p,\beta}$ is defined in the following way. Since E does not have complex multiplication, if p is ordinary, we can write $\omega_E = e_\alpha + e_\beta$ in $D \otimes \mathbf{Q}_p(\alpha)$ where e_α (resp. e_β) is an eigenvector of the Frobenius operator φ corresponding to the eigenvalue α^{-1} (resp. β^{-1}). Perrin-Riou constructed a map which interpolates the dual exponential map (cf. [18] Theorem 3.2.3, [9] Theorem 16.4) $\mathbf{H}^1_{\mathrm{loc}} \otimes_\Lambda \mathcal{H}_\infty \longrightarrow D \otimes_{\mathbf{Q}_p} \mathcal{H}_\infty$. The image of Kato's element z_K can be written as $\mathcal{L}_{p,\alpha} e_\alpha + \mathcal{L}_{p,\beta} e_\beta$ if p is supersingular, and the e_α component of the image of z_K is $\mathcal{L}_{p,\alpha}$ in the ordinary case. We simply define $\mathcal{L}_{p,\beta}$ by $z_K \mapsto \mathcal{L}_{p,\alpha} e_\alpha + \mathcal{L}_{p,\beta} e_\beta$ in the ordinary case.

Set

$$r = \min\{\mathrm{ord}_{T=0}\, \mathcal{L}_{p,\alpha}, \mathrm{ord}_{T=0}\, \mathcal{L}_{p,\beta}\}.$$

We conjecture that if $r > 0$,

$$\frac{\mathcal{L}^{(r)}_{p,\alpha}(0)}{(1-\frac{1}{\alpha})^2} \neq \frac{\mathcal{L}^{(r)}_{p,\beta}(0)}{(1-\frac{1}{\beta})^2} \tag{6}$$

which is equivalent to Conjecture 0.2 in the case $a_p = 0$. Note that if $r = 0$, we have

$$\frac{\mathcal{L}_{p,\alpha}(0)}{(1-\frac{1}{\alpha})^2} = \frac{\mathcal{L}_{p,\beta}(0)}{(1-\frac{1}{\beta})^2} = \frac{L(E,1)}{\Omega_E}.$$

So the above conjecture (6) asserts that $\mathcal{L}^{(r)}_{p,\alpha}(0)/(1-\alpha^{-1})^2 = \mathcal{L}^{(r)}_{p,\beta}(0)/(1-\beta^{-1})^2$ if and only if $r = 0$.

We remark that the p-adic Birch and Swinnerton-Dyer conjecture would imply $r = \mathrm{ord}_{T=0}\, \mathcal{L}_{p,\alpha} = \mathrm{ord}_{T=0}\, \mathcal{L}_{p,\beta}$, but if we had $\mathrm{ord}_{T=0}\, \mathcal{L}_{p,\alpha} \neq \mathrm{ord}_{T=0}\, \mathcal{L}_{p,\beta}$, Conjecture (6) would follow automatically. The p-adic Birch and Swinnerton-Dyer conjecture predicts

$$\left(\frac{d}{ds}\right)^r \mathcal{L}_{p,\alpha}(\kappa(\gamma)^{s-1} - 1)\big|_{s=1} = \left(1 - \frac{1}{\alpha}\right)^2 \frac{\#Ш(E/\mathbf{Q})\, \mathrm{Tam}(E/\mathbf{Q})}{(\#E(\mathbf{Q})_{\mathrm{tors}})^2} R_{p,\alpha}$$

(cf. Colmez [4]) where $\kappa : \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}) \longrightarrow \mathbf{Z}_p^\times$ is the cyclotomic character, and $R_{p,\alpha}$ (resp. $R_{p,\beta}$) is the p-adic α-regulator (β-regulator) of E. Hence, if we admit this conjecture, Conjecture (6) means that $R_{p,\alpha} \neq R_{p,\beta}$.

We now establish that $\mathcal{L}^{(r)}_{p,\alpha}(0)/(1-\alpha^{-1})^2 \neq \mathcal{L}^{(r)}_{p,\beta}(0)/(1-\beta^{-1})^2$ implies that $\#\,\mathrm{Sel}(E/\mathbf{Q})_{p^\infty} = \infty$. Namely, Conjecture (6) implies Conjecture 0.1. We know $(\mathbf{H}^1_{\mathrm{glob}})_{\mathbf{Q}} = \mathbf{H}^1_{\mathrm{glob}} \otimes \mathbf{Q}$ is a free $\Lambda_{\mathbf{Q}} = \Lambda \otimes \mathbf{Q}$-module of rank 1 (Kato [9] Theorem 12.4). Suppose that T^s divides Kato's element z_K and T^{s+1} does not divide z_K in $(\mathbf{H}^1_{\mathrm{glob}})_{\mathbf{Q}}$. We denote by ξ_i the image of z_K/T^i in $H^1(\mathbf{Q}, V)$ for $i = 1, ..., s$. Clearly, $\xi_1 = ... = \xi_{s-1} = 0$, and $\xi_s \neq 0$ because the

natural map $(\mathbf{H}^1_{\mathrm{glob}})_{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})}\otimes\mathbf{Q}\longrightarrow H^1(\mathbf{Q},V)$ is injective ($(\mathbf{H}^1_{\mathrm{glob}})_{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})}$ is the $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$-coinvariants of $\mathbf{H}^1_{\mathrm{glob}}$). We assume $\mathcal{L}^{(r)}_{p,\alpha}(0)/(1-\alpha^{-1})^2\neq\mathcal{L}^{(r)}_{p,\beta}(0)/(1-\beta^{-1})^2$, which implies that $L(E,1)=0$. We will show that the image of ξ_s in $H^1(\mathbf{Q}_p,V)$ is in $H^1_f(\mathbf{Q}_p,V)=E(\mathbf{Q}_p)\otimes\mathbf{Q}_p$. Put $D^0=\mathbf{Q}_p\omega_E$ and

$$L(i)=(1-\alpha^{-1})^{-2}\mathcal{L}^{(i)}_{p,\alpha}(0)e_\alpha+(1-\beta^{-1})^{-2}\mathcal{L}^{(i)}_{p,\beta}(0)e_\beta\in D.$$

We know that the image of ξ_i by $\exp^*$ is $L(i)$ times a non-zero element, and if ξ_i is in $H^1_f(\mathbf{Q}_p,V)$, the image of ξ_i by $\log: H^1_f(\mathbf{Q}_p,V)\longrightarrow D/D^0$ is $L(i+1)$ times a non-zero element modulo D^0 by Perrin-Riou's formulas [17] Propositions 2.1.4 and 2.2.2. (Note that Conjecture Réc(V) in [17] was proved by Colmez [3].)

Suppose that $r\leq s$. By our assumption, $L(r)$ is not in D^0, hence $\log(\xi_{r-1})$ is not in D^0. Thus, ξ_{r-1} is a non-zero element in $H^1(\mathbf{Q}_p,V)$. But this is a contradiction because $\xi_{r-1}=0$ in $H^1(\mathbf{Q},V)$ by the definition of s. Thus, we have $r>s$. This implies that $L(s)=0$, and hence, $\exp^*(\xi_s)=0$. So ξ_s is in $H^1_f(\mathbf{Q}_p,V)$. Therefore, ξ_s is in the Selmer group $\mathrm{Sel}(E/\mathbf{Q},V)$ with respect to V, and $\#\,\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}=\infty$. This can be also obtained from Proposition 4.10 in Perrin-Riou [19].

Next, we will show that $\mathrm{rank}\,E(\mathbf{Q})>0$ and $(*)_0$ imply (6). These conditions imply that ξ_s is in $H^1_f(\mathbf{Q}_p,V)$ (by Lemma 1.4), and also is non-zero. Therefore, $L(s+1)$ is not in D^0. This shows that $r=s+1$ and (6) holds.

2 Constructing a rational point in $E(\mathbf{Q})$

We saw in the previous section that the value $(f/g)(0)-(p-1)/2$ is important to understand the Selmer group. In this section, we consider the case $r=\mathrm{ord}_{T=0}\,f(T)=\mathrm{ord}_{T=0}\,g(T)=1$. We will see that the computation of the value $f'(0)-\frac{p-1}{2}g'(0)$ helps to produce a rational point in $E(\mathbf{Q})$ numerically. To do this, we have to compute the value $f'(0)-\frac{p-1}{2}g'(0)$ to high accuracy, which we do using the theory of overconvergent modular symbols.

2.1. Overconvergent modular symbols. Let Δ_0 denote the space of degree zero divisors on $\mathbf{P}^1(\mathbf{Q})$ which naturally are a left $\mathrm{GL}_2(\mathbf{Q})$-module under linear fractional transformations. Let $\Sigma_0(p)$ be the semigroup of matrices $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in M_2(\mathbf{Z}_p)$ such that p divides c, $\gcd(a,p)=1$ and $ad-bc\neq 0$. If V is some right $\mathbf{Z}_p[\Sigma_0(p)]$-module, then the space $\mathrm{Hom}(\Delta_0,V)$ is naturally a right $\Sigma_0(p)$-module by

$$(\varphi\big|\gamma)(D)=\varphi(\gamma D)\big|\gamma.$$

For a congruence subgroup $\Gamma \subset \Gamma_0(p) \subset \mathrm{SL}_2(\mathbf{Z})$, we set

$$\mathrm{Symb}_\Gamma(V) = \left\{\varphi \in \mathrm{Hom}(\Delta_0, V) \ : \ \varphi\big|\gamma = \varphi\right\},$$

the subspace of Γ-invariant maps which we refer to as the space of *V-valued modular symbols of level Γ*.

We note that this space is naturally a Hecke module. For instance, U_p is defined by $\sum_{a=1}^{p-1}\left(\begin{smallmatrix}1 & a\\ 0 & p\end{smallmatrix}\right)$. Also, the action of the matrix $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ decomposes $\mathrm{Symb}_\Gamma(V)$ into plus/minus subspaces $\mathrm{Symb}_\Gamma(V)^\pm$.

If we take $V = \mathbf{Q}_p$, $\mathrm{Symb}_\Gamma(\mathbf{Q}_p)$ is the classical space of modular symbols of level Γ over $\mathbf{Q}_p$. By Eichler-Shimura theory, each eigenform f over $\mathbf{Q}_p$ of level Γ gives rise to an eigensymbol $\varphi_f^\pm$ in $\mathrm{Symb}_\Gamma(\mathbf{Q}_p)^\pm$ with the same Hecke-eigenvalues as f.

Let $\mathcal{D}(\mathbf{Z}_p)$ denote the space of (locally analytic) distributions on $\mathbf{Z}_p$. Then $\mathcal{D}(\mathbf{Z}_p)$ inherits a right $\Sigma_0(p)$-action defined by:

$$(\mu|\gamma)(f(x)) = \mu\left(f\left(\frac{b+dx}{a+cx}\right)\right).$$

Then $\mathrm{Symb}_\Gamma(\mathcal{D}(\mathbf{Z}_p))$ is Steven's space of *overconvergent modular symbols*. This space admits a Hecke-equivariant map to the space of classical modular symbols

$$\rho : \mathrm{Symb}_\Gamma(\mathcal{D}(\mathbf{Z}_p)) \longrightarrow \mathrm{Symb}_\Gamma(\mathbf{Q}_p)$$

by taking total measure. That is, $\rho(\Phi)(D) = \Phi(D)(\mathbf{1}_{\mathbf{Z}_p})$. We refer to this map as the *specialization* map.

Theorem 2.1 (Stevens) *The operator U_p is completely continuous on $\mathrm{Symb}_\Gamma(\mathcal{D}(\mathbf{Z}_p))$. Moreover, the Hecke-equivariant map*

$$\rho : \mathrm{Symb}_\Gamma(\mathcal{D}(\mathbf{Z}_p))^{(<1)} \xrightarrow{\sim} \mathrm{Symb}_\Gamma(\mathbf{Q}_p)^{(<1)}$$

is an isomorphism. Here the superscript (<1) refers to the subspace where U_p acts with slope less than 1.

See [26] Theorem 7.1 for a proof of this theorem.

2.2. Connection to p-adic L-functions. Now consider an elliptic curve $E/\mathbf{Q}$ of level N with good supersingular reduction at p. By the Modularity theorem, there is some modular form $f = f_E$ on $\Gamma_0(N)$ corresponding to E. If α is a root of $x^2 - a_p x + p = 0$, let $f_\alpha(\tau) = f(\tau) + \alpha f(p\tau)$ denote the p-stabilization of f to level $\Gamma_0(Np)$. By Eichler-Shimura theory, there exists

a Hecke-eigensymbol $\varphi_{f,\alpha} = \varphi^+_{f,\alpha} \in \mathrm{Symb}_\Gamma(\mathbf{Q}_p)^+ \otimes \mathbf{Q}_p(\alpha)$ with the same Hecke-eigenvalues as f_α. Explicitly, we have

$$\varphi^+_{f,\alpha}(\{r\} - \{s\}) = \pi i \left(\int_s^r f_\alpha + \int_{-s}^{-r} f_\alpha \right) \Omega_E^{-1}$$

where Ω_E is the Néron period of $E/\mathbf{Q}$.

By Stevens' comparison theorem (Theorem 2.1), there exists a unique overconvergent Hecke-eigensymbol $\Phi_\alpha = \Phi^+_\alpha \in \mathrm{Symb}_\Gamma(\mathcal{D}(\mathbf{Z}_p))^+ \otimes \mathbf{Q}_p(\alpha)$ such that $\rho(\Phi_\alpha) = \varphi_{f,\alpha}$. (Note that since $\varphi_{f,\alpha}\big|U_p = \alpha \cdot \varphi_{f,\alpha}$, the symbol $\varphi_{f,\alpha}$ has slope $1/2$ and the theorem applies.)

The overconvergent symbol Φ_α is intimately connected to the p-adic L-function of E. Indeed,

$$\Phi_\alpha(\{0\} - \{\infty\}) = L_{p,\alpha}(E), \tag{7}$$

the p-adic L-function of E viewed as a (locally analytic) distribution on $\mathbf{Z}_p^\times$. To verify this, one uses the fact that Φ_α lifts $\varphi_{f,\alpha}$, that $\Phi_\alpha\big|U_p = \alpha \cdot \Phi_\alpha$ and that, by definition,

$$L_{p,\alpha}(E)(\mathbf{1}_{a+p^n\mathbf{Z}_p}) = \tfrac{1}{\alpha^n} \cdot \varphi_{f,\alpha}\left(\left\{ \tfrac{a}{p^n} \right\} - \{\infty\} \right).$$

See [26] Theorem 8.3.

2.3. Computing p-adic L-functions. As in [21] and [6], one can use the theory of overconvergent modular symbols to very efficiently compute the p-adic L-function of an elliptic curve. Indeed, by (7), it suffices to compute the corresponding overconvergent modular symbol Φ_α.

To do this, we first lift $\varphi_{f,\alpha}$ to any overconvergent symbol Φ (not necessarily a Hecke-eigensymbol). Then, using Theorem 2.1, one can verify that the sequence $\{\alpha^{-n}\Phi\big|U_p^n\}$ converges to Φ_α. Thus, as long as we can efficiently compute U_p on spaces of overconvergent modular symbols, we can form approximations to the symbol Φ_α.

To actually perform such a computation, one must work modulo various powers of p and thus we must make a careful look at the denominators that are present. If $\mathcal{O}$ denotes the ring of integers of $\mathbf{Q}_p(\alpha)$, then $\varphi_{f,\alpha} \in \frac{1}{\alpha}\mathrm{Symb}_\Gamma(\mathbf{Z}_p)$. (The factor of $\frac{1}{\alpha}$ comes about from the p-stabilization of f from level N to level Np.) Let $\mathcal{D}^0(\mathbf{Z}_p)$ denote the set of distributions whose moments are all integral; that is,

$$\mathcal{D}^0(\mathbf{Z}_p) = \{\mu \in \mathcal{D}(\mathbf{Z}_p) : \mu(x^j) \in \mathbf{Z}_p\}.$$

It is then possible to lift $\varphi_{f,\alpha}$ to a symbol Φ in $\frac{1}{\alpha^2}\mathrm{Symb}_\Gamma(\mathcal{D}^0(\mathbf{Z}_p)) \otimes \mathcal{O}$.

As mentioned above, $\{\alpha^{-n}\Phi\big|U_p^n\}$ converges to Φ_α. However, the space $\mathrm{Symb}_\Gamma(\mathcal{D}^0(\mathbf{Z}_p)) \otimes \mathcal{O}$ is not preserved by the operator $\frac{1}{\alpha}U_p$. However, the subspace

$$X := \left\{\Phi \in \mathrm{Symb}_\Gamma(\mathcal{D}^0(\mathbf{Z}_p)) \otimes \mathcal{O} : \rho(\Phi)\big|U_p = \alpha\rho(\Phi) \text{ and } \rho(\Phi) \in \alpha\mathrm{Symb}_\Gamma(\mathcal{O})\right\}$$

is preserved by $\frac{1}{\alpha}U_p$. (Note that the two conditions defining this set are clearly preserved by this operator. The key point here is that overconvergent symbols with *integral* moments satisfying these two conditions will still have integral moments after applying $\frac{1}{\alpha}U_p$.)

Thus, to form our desired overconvergent symbol using only symbols with integral moments, we begin with $\alpha^2\varphi_{f,\alpha} \in \alpha\mathrm{Symb}_\Gamma(\mathcal{O})$ and lift this symbol to an overconvergent symbol Φ' in X. Then $\frac{1}{\alpha^n}\Phi'\big|U_p^n$ is in X for all n and converges to $\alpha^2\Phi_\alpha$.

To perform this computation on a computer, we need a method of approximating an overconvergent modular symbol with a finite amount of data. Furthermore, we must ensure that our approximations are stable under the action of $\Sigma_0(p)$ so that Hecke operators can be computed. A method of approximating distributions using "finite approximation modules" is given in [21] and [6] Section 2.4 which we will now describe.

Consider the set

$$\mathcal{F}(M) = \mathcal{O}/p^M \times \mathcal{O}/p^{M-1} \times \cdots \times \mathcal{O}/p.$$

We then have a map

$$\mathcal{D}^0(\mathbf{Z}_p) \otimes \mathcal{O} \longrightarrow \mathcal{F}(M) \text{ given by } \mu \mapsto \{\mu(x^j) \bmod p^{M-j}\}_{j=0}^{M-1}.$$

Moreover, one can check that the kernel of this map is stable under the action of $\Sigma_0(p)$. This allows us to give $\mathcal{F}(M)$ the structure of a $\Sigma_0(p)$-module.

As $\mathcal{F}(M)$ is a finite set, the space $\mathrm{Symb}_\Gamma(\mathcal{F}(M))$ can be represented on a computer. Indeed, there is a finite set of divisors such that any modular symbol of level Γ is uniquely determined by its values on these divisors. Thus, any element of $\mathrm{Symb}_\Gamma(\mathcal{F}(M))$ can be represented by a finite list of elements in $\mathcal{F}(M)$.

Moreover, since

$$\mathrm{Symb}_\Gamma(\mathcal{D}^0(\mathbf{Z}_p)) \otimes \mathcal{O} \cong \varprojlim \mathrm{Symb}_\Gamma(\mathcal{F}(M)),$$

these spaces provide a natural setting to perform computations with overconvergent modular symbols.

To compute the p-adic L-function of E, we fix some large integer M and consider the image of $\alpha^2\varphi_{f,\alpha}$ in $\mathrm{Symb}_\Gamma(\mathcal{O}/p^M)$. One can explicitly lift this symbol to a symbol $\overline{\Phi}'$ in $\mathrm{Symb}_\Gamma(\mathcal{F}(M))$. (See [21] for explicit formulas related to such liftings.)

In the ordinary case, one then proceeds by simply computing the sequence $\{\alpha^{-n}\overline{\Phi}'\big|U_p^n\}$ which will eventually stabilize to the image of $\alpha^2\Phi_\alpha$ in $\mathrm{Symb}_\Gamma(\mathcal{F}(M))$.

However, in the supersingular case, α is not a unit and thus division by α causes a loss of accuracy. The symbol $\alpha^{-2n}\overline{\Phi}'\big|U_p^{2n}$ is naturally a symbol in $\mathcal{F}(M-n)$ and is congruent to $\alpha^2\Phi_\alpha$ modulo p^n. By choosing M and n appropriately, one can then produce a U_p-eigensymbol to any given desired accuracy.

2.4. Twists. Let χ_d denote the quadratic character of conductor d and let E_d be the quadratic twist of E by χ_d. Let $\alpha^* = \chi_d(p)\alpha$ and let Φ_α be the overconvergent eigensymbol whose special value at $\{0\}-\{\infty\}$ equals $L_{p,\alpha}(E)$. If $\gcd(d, Np) = 1$, then

$$\Phi_{\alpha^*,d} := \sum_{a=1}^{|d|} \chi_d(a)\cdot \Phi_\alpha\Big|\begin{pmatrix}1 & \frac{a}{d}\\ 0 & 1\end{pmatrix}$$

is a U_p-eigensymbol of level $\Gamma_0(d^2Np)$ with eigenvalue α^*. Moreover, if $d > 0$, then

$$\Phi_{\alpha^*,d}\left(\{0\}-\{\infty\}\right) = L_{p,\alpha^*}(E_d).$$

In particular, once we have constructed an eigensymbol that computes $L_{p,\alpha}(E)$, we can use this symbol to compute the p-adic L-function of all real quadratic twists of E. (To compute imaginary quadratic twists one needs to instead use the overconvergent symbol that corresponds to $\varphi^-_{f,\alpha}$.)

2.5. Computing derivatives of p-adic L-functions. Once the image of Φ_α has been computed in $\mathrm{Symb}_\Gamma(\mathcal{F}(M))$ for some M, by evaluating at $D = \{0\}-\{\infty\}$ we can recover the first M moments of the p-adic L-function modulo certain powers of p. As in [6] pg. 17, we can also recover

$$\int_{a+p\mathbf{Z}_p} (x-\{a\})^j\, dL_{p,\alpha}(E) \mod p^M$$

for $0 \le j \le M-1$ where $\{a\}$ denotes the Teichmüller lift of a.

Using these values one can compute the derivative of this p-adic L-function. Indeed, if we let $L_{p,\alpha}(E,s)$ be the function of $L_{p,\alpha}(E)$ in the s-

variable, then

$$\begin{aligned} L'_{p,\alpha}(E,s)\Big|_{s=1} &= \int_{\mathbf{Z}_p^\times} \log_p(x)\ dL_{p,\alpha}(E) \\ &= \sum_{a=1}^{p-1} \int_{a+p\mathbf{Z}_p} \log_p(x/\{a\})\ dL_{p,\alpha}(E) \\ &= \sum_{a=1}^{p-1} \int_{a+p\mathbf{Z}_p} \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j}(x/\{a\}-1)^j\ dL_{p,\alpha}(E) \\ &= \sum_{a=1}^{p-1} \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j}\{a\}^{-j} \int_{a+p\mathbf{Z}_p} (x-\{a\})^j\ dL_{p,\alpha}(E). \end{aligned}$$

Since $\int_{a+p\mathbf{Z}_p}(x-\{a\})^j\ dL_{p,\alpha}(E)$ is divisible by p^j, by calculating the above expression for j between 0 and $M-1$, one obtains an approximation to $L'_{p,\alpha}(E,1)$ which is correct modulo p^{M-r} where $p^r \le M < p^{r+1}$.

Let $\mathcal{L}_{p,\alpha}(T)$ be the p-adic L-function in the T-variable as in §1. Then $\mathcal{L}_{p,\alpha}(\kappa(\gamma)^{s-1}-1) = L_{p,\alpha}(E,s)$, and $\mathcal{L}_{p,\alpha}(T) = f(T)\log^+(T) + g(T)\log^-(T)\alpha$. Hence,

$$\begin{aligned} L'_{p,\alpha}(E,s)\Big|_{s=1} &= \mathcal{L}'_{p,\alpha}(T)\Big|_{T=0} \cdot \log(\kappa(\gamma)) \\ &= \big(f'(0)\log^+(0) + g'(0)\log^-(0)\alpha\big)\cdot\log(\kappa(\gamma)) \\ &= \frac{1}{p}\cdot(f'(0)+g'(0)\alpha)\cdot\log(\kappa(\gamma)). \end{aligned} \tag{8}$$

So from the computation of the derivative of $L_{p,\alpha}(E,s)$, we can easily compute the values of $f'(0)$ and $g'(0)$.

2.6. p-adic Birch and Swinnerton-Dyer conjecture. We now give a precise statement of the p-adic Birch and Swinnerton-Dyer conjecture as in Bernardi and Perrin-Riou [1]. As before, $E/\mathbf{Q}$ is an elliptic curve for which p is a good supersingular prime with $a_p = 0$. If r is the order of $L_{p,\alpha}(E/\mathbf{Q},s)$ at $s=1$, then this conjecture asserts that $r = \operatorname{rank} E(\mathbf{Q})$ and

$$\frac{1}{r!}L^{(r)}_{p,\alpha}(E/\mathbf{Q},s)\big|_{s=1} = \left(1-\frac{1}{\alpha}\right)^2 C_p(E/\mathbf{Q})\cdot R_{p,\alpha}(E/\mathbf{Q}) \tag{9}$$

where $R_{p,\alpha}(E/\mathbf{Q})$ is the p-adic α-regulator of $E/\mathbf{Q}$, and

$$C_p(E/\mathbf{Q}) = \frac{\#Ш(E/\mathbf{Q})\cdot \operatorname{Tam}(E/\mathbf{Q})}{(\#E(\mathbf{Q})_{\mathrm{tors}})^2}$$

(cf. also [4], [19]). In the case $r = 1$, we have

$$R_{p,\alpha}(E/\mathbf{Q}) = -\frac{1}{[\varphi(\omega_E), \omega_E]} \cdot \left(h_{\varphi(\omega_E)}(P) + \frac{h_{\omega_E}(P)}{p}\alpha \right) \tag{10}$$

where P is some generator of $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}}$, and ω_E, φ, $[\varphi(\omega_E), \omega_E]$ are as in §1. Here, for each $\nu \in D = D_{dR}(V_p(E))$, there is a p-adic height function $h_\nu : E(\mathbf{Q}) \longrightarrow \mathbf{Q}_p$ attached to ν. If $\nu = \omega_E$ and if P is in the kernel of reduction modulo p, then $h_{\omega_E}(P) = -\log_{\hat{E}}(P)^2$ where $\log_{\hat{E}} : \hat{E}(\mathbf{Q}_p) \longrightarrow \mathbf{Q}_p$ is the logarithm of the formal group $\hat{E}/\mathbf{Q}_p$ attached to E.

Assuming the p-adic Birch and Swinnerton-Dyer conjecture (with $r = 1$), equations (8), (9) and (10) yield

$$\begin{aligned}
&\left(1 - \frac{1}{\alpha}\right)^{-2} (f'(0) + g'(0)\alpha) \log(\kappa(\gamma)) \\
&\qquad = \frac{p(p-1) - 2p\alpha}{(p+1)^2} (f'(0) + g'(0)\alpha) \log(\kappa(\gamma)) \\
&\qquad = -\frac{p}{[\varphi(\omega_E), \omega_E]} \cdot \left(h_{\varphi(\omega_E)}(P) + \frac{h_{\omega_E}(P)}{p}\alpha \right) C_p(E/\mathbf{Q}).
\end{aligned}$$

Equating α-coefficients of both sides gives

$$\frac{2p \log(\kappa(\gamma))}{(p+1)^2} \cdot \left(f'(0) - \frac{p-1}{2} g'(0) \right) = \frac{h_{\omega_E}(P) \cdot C_p(E/\mathbf{Q})}{[\varphi(\omega_E), \omega_E]}.$$

Since $\hat{E}(\mathbf{Q}_p) = E^1(\mathbf{Q}_p)$ is the kernel of the reduction map $E(\mathbf{Q}_p) \longrightarrow E(\mathbf{F}_p)$, $(E(\mathbf{Q}_p) : \hat{E}(\mathbf{Q}_p)) = \#E(\mathbf{F}_p) = p + 1$, and $(p+1)P$ is in $\hat{E}(\mathbf{Q}_p)$. The above formula can be written as

$$\log_{\hat{E}}\left((p+1)P\right)^2 = -\frac{f'(0) - \frac{p-1}{2} g'(0)}{C_p(E/\mathbf{Q})} 2p \log(\kappa(\gamma))[\varphi(\omega_E), \omega_E]. \tag{11}$$

Note that the fact that we have two p-adic L-functions which are computable, gives us the advantage that $\log_{\hat{E}}((p+1)P)$ is expressed by computable terms.

We apply this formula to a quadratic twist of E, and have a twisted version of this equation. Let $\mathcal{L}_{p,\alpha^*}(E_d, T)$ be the function in the T-variable corresponding to $L_{p,\alpha^*}(E_d)$ defined in 2.4. We assume that the rank of $E_d(\mathbf{Q})$ equals 1 and P_d is a generator of the Mordell-Weil group modulo torsion. Also, we define $f_d(T)$ and $g_d(T)$ by

$$\mathcal{L}_{p,\alpha^*}(E_d, T) = f_d(T) \log^+(T) + g_d(T) \log^-(T) \alpha^*.$$

Then, we have a twisted equation

$$\log_{\hat{E}_d}((p+1)P_d)^2 = -\frac{\eta_d^2\left(f_d'(0) - \frac{p-1}{2}g_d'(0)\right)}{d\cdot C_p(E_d/\mathbf{Q})}2p\log(\kappa(\gamma))[\varphi(\omega_E),\omega_E]. \quad (12)$$

Here, η_d is defined by $\omega_{E_d} = \frac{\eta_d}{\sqrt{d}}\omega_E$. (Note that η_d is written down explicitly in [1] pg. 230. In most cases, $\eta_d = 1$.)

2.7. Computing rational points. Using equation (11) we can attempt to use the p-adic L-function to p-adically compute global points on $E(\mathbf{Q})$. Suppose that we do not know $Ш(E/\mathbf{Q})$. We first compute

$$z_p(E) = \exp_{\hat{E}}\left(\sqrt{-\frac{\left(f'(0) - \frac{p-1}{2}g'(0)\right)2p\log(\kappa(\gamma))[\varphi(\omega_E),\omega_E]}{\mathrm{Tam}(E)}}\cdot\frac{\#E(\mathbf{Q})_{\mathrm{tors}}}{p+1}\right) \quad (13)$$

where $\exp_{\hat{E}}$ is the inverse of $\log_{\hat{E}}$ (the formal exponential of $\hat{E}$). The quantity in the parentheses should be in $p\mathbf{Z}_p$ because of the p-adic Birch and Swinnerton-Dyer conjecture (cf. (11)), so the right hand side should converge. If $\hat{x}(t)$, $\hat{y}(t)$ represent the formal x and y coordinate functions of $\hat{E}/\mathbf{Q}_p$, then

$$\tilde{P}' := (\hat{x}(z_p(E)), \hat{y}(z_p(E)))$$

is a point in $\hat{E}(\mathbf{Q}_p)$. The p-adic Birch and Swinnerton-Dyer conjecture (11) predicts that there is a global point $P' \in E(\mathbf{Q})$ such that

$$(p+1)P' = (p+1)\tilde{P}' \text{ in } E(\mathbf{Q}_p).$$

(The point P' should be $\sqrt{\#Ш(E/\mathbf{Q})}P$ in the terminology of (11)). Thus, there is a point $Q \in E(\mathbf{Q}_p)$ of order dividing $p+1$ such that $P' = \tilde{P}' + Q$. So we can proceed in the following way. We first compute p-adically all Q of order dividing $p+1$ in $E(\mathbf{Q}_p)$. Then, for each such Q, we check to see if $\tilde{P}' + Q$ appears to be a global point.

2.8. Computing in practice. We explain our method in the case of computing points on a quadratic twist of E. Considering (12), we define

$$z_p(E,d) := \quad (14)$$
$$\exp_{\hat{E}}\left(\sqrt{-\frac{\left(f_d'(0) - \frac{p-1}{2}g_d'(0)\right)\cdot 2p\log(\kappa(\gamma))[\varphi(\omega_E),\omega_E]}{d\,\mathrm{Tam}(E_d)}}\cdot\frac{\eta_d\#E_d(\mathbf{Q})_{\mathrm{tors}}}{p+1}\right),$$

and

$$\tilde{P}'_d := (\hat{x}(z_p(E,d)), \hat{y}(z_p(E,d))).$$

To carry out this computation, we need to first get a good p-adic approximation of $z_p(E,d)$ and thus a p-adic approximation of $\tilde{P}'_d$. Then, we compute p-adic approximations of the $(p+1)$-torsion in $E_d(\mathbf{Q}_p)$. To find a global point, we translate $\tilde{P}'_d$ around by these torsion points with the hope of finding some rational point that is very close p-adically to one of these translates. Fortunately, if we find a candidate global point, we can simply go back to the equation of E_d to see if the point actually sits on our curve.

The key terms that need to be computed in order to determine $\tilde{P}'_d$ are $f'_d(0)$, $g'_d(0)$, $\exp_{\hat{E}}(t)$, $\hat{x}(t)$, $\hat{y}(t)$, $\mathrm{Tam}(E_d/\mathbf{Q})$, $\#E_d(\mathbf{Q})_{\mathrm{tors}}$, and $[\varphi(\omega_E), \omega_E]$. The most difficult of these terms to compute are $f'_d(0)$ and $g'_d(0)$. We cannot use Riemann sums to approximate $f'_d(0)$ and $g'_d(0)$, since in practice we will need a fairly high level of p-adic accuracy in order to recognize global points. (To get n digits of p-adic accuracy, one needs to sum together approximately p^n modular symbols which becomes implausible for large n.) Instead, we use the theory of overconvergent modular symbols explained above to compute $f'_d(0)$ and $g'_d(0)$ to high accuracy.

For the remaining terms, computing invariants of the formal group $\hat{E}/\mathbf{Q}_p$ is standard. (We used the package [25].) The arithmetic invariants ($\mathrm{Tam}(E_d/\mathbf{Q})$ and $\#E_d(\mathbf{Q})_{\mathrm{tors}}$) of the elliptic curve E_d are easy to compute. (We used the intrinsic functions of MAGMA [14].)

Lastly, an algorithm to compute $[\varphi(\omega_E), \omega_E]$ is outlined in [1] pg. 232. However, we sidestepped this issue in the following way. For one particular twist E_d with $Ш(E_d/\mathbf{Q}) = 0$, we found a generator P_d of $E_d(\mathbf{Q})/E_d(\mathbf{Q})_{\mathrm{tors}}$ directly using `mwrank` [5]. Then, using (11), we can determine what the value of $[\varphi(\omega_E), \omega_E]$ should be to high accuracy since every other expression in (11) is computable to high accuracy. (We actually repeated this computation for several different twists to make sure that the predicted value of $[\varphi(\omega_E), \omega_E]$ was always the same.)

Lastly, to recognize the coordinates of $\tilde{P}'_d$ as rational numbers, we used the method of rational reconstruction as explained in [11] and, in practice, we used the recognition function in [7].

2.9. The computations. We performed the above described computations for the curves $X_0(17)$ and $X_0(32)$ and the prime $p = 3$. (These computations were done on William Stein's meccah cluster.) For $X_0(17)$ (resp. $X_0(32)$) we computed the associated overconvergent symbol Φ_α modulo 3^{200} (resp. 3^{100}). Because of the presence of the square root in (14), we then were only able to compute $\tilde{P}_d$ to 100 (resp. 50) 3-adic digits for $X_0(17)$ (resp. $X_0(32)$).

For $X_0(17)$ (resp. $X_0(32)$), we could find a global point on all quadratic twists $0 < d < 250$ except for $d = 197$ (resp. $0 < d < 150$) with $\gcd(d, 3N) = 1$. (For $X_0(17)_{197}$ one could find a point via several different methods, but our method would require a more accurate computation of overconvergent modular symbols.) We made a table of these points in §4.

Another interesting example whose d is not in the above mentioned range is $E_d = X_0(17)_d$ with $d = 328$. We found a global point $P' = (28069/25, 3626247/125)$ on the curve

$$E_{328} : y^2 = x^3 - 73964x - 490717520$$

by the method which we described above. We also computed

$$\text{“}\frac{1}{2}\text{”} z_p(E, d) := \exp_{\hat{E}} \left(\frac{1}{2} \sqrt{ - \frac{\left(f_d'(0) - \frac{p-1}{2} g_d'(0) \right) \cdot 2p \log(\kappa(\gamma))[\varphi(\omega_E), \omega_E]}{d \operatorname{Tam}(E_d)} } \cdot \frac{\eta_d \# E_d(\mathbf{Q})_{\text{tors}}}{p+1} \right).$$

From this local point, we produced a global point $P = (1398, -46240)$ on the curve E_{328}. This reflects well the fact that $\#Ш(E/\mathbf{Q}) = 4$ in this case. The point $P = (1398, -46240)$ should be a generator of $E(\mathbf{Q})$ modulo torsion.

3 The structure of fine Selmer groups and the gcd of $f(T)$ and $g(T)$

In this section, we will study the problem mentioned in §0.3, and the greatest common divisor of $f(T)$ and $g(T)$.

3.1. Greenberg's "conjecture" (problem). Suppose that $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)$, e_n, $f(T)$, $g(T)$, ... are as in §0.3. As we explained in §0.3, we are interested in the following problem (conjecture) by Greenberg.

Problem 0.7

$$\operatorname{char}(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = (\prod_{\substack{e_n \geq 1 \\ n \geq 0}} \Phi_n^{e_n - 1}).$$

First of all, since $E(\mathbf{Q}_{p,n}) \otimes \mathbf{Q}_p$ is a one dimensional regular representation of $G_n = \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$, by the definition of e_n, $\mathrm{Ker}(E(\mathbf{Q}_n) \otimes \mathbf{Q}_p \longrightarrow E(\mathbf{Q}_{p,n}) \otimes$

$\mathbf{Q}_p$) contains $(\mathbf{Q}_p[T]/\Phi_n(T))^{e_n-1}$ if $e_n \geq 1$. Hence, $\mathrm{Sel}_0(E/\mathbf{Q}_n)$ contains $((\mathbf{Z}_p[T]/\Phi_n(T)) \otimes \mathbf{Q}_p/\mathbf{Z}_p)^{e_n-1}$, and we always have

$$\mathrm{char}(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) \subset (\prod_{\substack{e_n \geq 1 \\ n \geq 0}} \Phi_n^{e_n-1}).$$

Coates and Sujatha conjectured in [2] that $\mu(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = 0$. In fact, they showed that $\mu^{class}_{\mathbf{Q}(E[p])} = 0$ implies $\mu(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = 0$ ([2] Theorem 3.4) where $\mu^{class}_{\mathbf{Q}(E[p])}$ is the classical Iwasawa μ-invariant for the class group of cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}(E[p])$ which is the field obtained by adjoining all p-torsion points of E. The proof of this fact can be described simply and slightly differently from [2], so we give here the proof. Put $F = \mathbf{Q}(E[p])$, and denote by F_∞/F the cyclotomic $\mathbf{Z}_p$-extension. By Iwasawa [8] Theorem 2, $\mu^{class}_F = 0$ implies $H^2(O_{F_\infty}[1/S], \mathbf{Z}/p\mathbf{Z}) = H^2_{et}(\mathrm{Spec}\, O_{F_\infty}[1/S], \mathbf{Z}/p\mathbf{Z}) = 0$ (S is the product of the primes of bad reduction and p). Hence, assuming $\mu^{class}_F = 0$, we have $H^2(O_{F_\infty}[1/S], E[p]) = 0$. Since the p-cohomological dimension of $\mathrm{Spec}\, O_{F_\infty}[1/S]$ is 2, the corestriction map $H^2(O_{F_\infty}[1/S], E[p]) \longrightarrow H^2(O_{\mathbf{Q}_\infty}[1/S], E[p])$ is surjective, so we get $H^2(O_{\mathbf{Q}_\infty}[1/S], E[p]) = 0$, which implies $\mu(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = 0$.

In the following, we assume p is supersingular and $a_p = 0$. As we explained in §0.3, a generator of $\mathrm{char}\,\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee$ divides both $f(T)$ and $g(T)$ (at least up to μ-invariants). Using this fact, we will prove what we mentioned in §0.3.

Proposition 3.1 *Assume that* $\mathrm{rank}\, E(\mathbf{Q}) = e_0$, $\min\{\lambda(f(T)), \lambda(g(T))\} = e_0$, *and* $\mu(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = 0$. *Then,* $\mathrm{char}\,\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee = (T^{e_0'})$ *where* $e_0' = \max\{0, e_0 - 1\}$, *and* Problem 0.7 *holds.*

Proof. Suppose, for example, $\lambda(f(T)) = e_0$. Since one divisibility of the main conjecture was proved (cf. 1.5), this assumption implies $(f(T)) = (T^{e_0})$ as ideals of Λ. If $e_0 = 0$, then $f(T)$ is a unit. Thus, $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)$ is finite and we get the conclusion. Hence, we may assume $e_0 > 0$. Then, $\mathrm{Sel}^-(E/\mathbf{Q}_\infty)^\vee \sim (\Lambda/(T))^{e_0}$ (pseudo-isomorphic), and by the control theorem for $\mathrm{Sel}^-(E/\mathbf{Q}_\infty)$ ([12] Theorem 9.3), $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ is of corank e_0. Since $E(\mathbf{Q}) \otimes \mathbf{Q}_p \longrightarrow E(\mathbf{Q}_p) \otimes \mathbf{Q}_p$ is surjective (because $e_0 > 0$), $\mathrm{Sel}_0(E/\mathbf{Q})$ is of corank $e_0 - 1$. By the control theorem for $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)$ (cf. [13] Remark 4.4), we get $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee \sim (\Lambda/(T))^{e_0-1}$, which implies the conclusion.

3.2. The gcd of $f(T)$ and $g(T)$.

We use the convention that we always express the greatest common divisor of elements in Λ of the form $p^\mu h(T)$ where $h(T)$ is a distinguished

polynomial. Concerning the greatest common divisor of $f(T)$ and $g(T)$, we propose

Problem 3.2
$$\gcd(f(T), g(T)) = T^{e_0} \prod_{\substack{e_n \geq 1 \\ n \geq 1}} \Phi_n^{e_n - 1}.$$

Proposition 3.3 *Assume* $\mu(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = 0$. *Then,* Problem 3.2 *implies* Problem 0.7.

We note that if we assume Problem 3.2, we have $\min\{\mu(f(T)), \mu(g(T))\} = 0$, hence if the Galois representation on the p-torsion points of E is surjective, $\mu(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = 0$ holds by [9] Theorem 13.4.

Proof of Proposition 3.3. As we explained in §0.3, $\mathrm{Sel}_0(E/\mathbf{Q}_\infty) \subset \mathrm{Sel}^{\pm}(E/\mathbf{Q}_\infty)$ which implies $\gcd(f(T), g(T)) \in \mathrm{char}(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee)$. So if Problem 3.2 is true, we have

$$(T^{e_0} \prod_{\substack{e_n \geq 1 \\ n \geq 1}} \Phi_n^{e_n - 1}) \subset \mathrm{char}(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) \subset (\prod_{\substack{e_n \geq 1 \\ n \geq 0}} \Phi_n^{e_n - 1}).$$

The rest of the proof is the same as that of Proposition 3.1. We may assume $e_0 > 0$. By the control theorem for $\mathrm{Sel}^{\pm}(E/\mathbf{Q}_\infty)$ ([12] Theorem 9.3) and our assumption that Problem 3.2 is true, $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ is of corank e_0. Hence, $\mathrm{Sel}_0(E/\mathbf{Q})$ is of corank $e_0 - 1$. Hence, if $\mathcal{F}$ is a generator of $\mathrm{char}(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee)$, by the control theorem for $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)$ (cf. [13] Remark 4.4), we have $\mathrm{ord}_T(\mathcal{F}) = e_0 - 1$. This implies that Problem 0.7 is true.

Next, we will assume Problem 0.7 and deduce Problem 3.2 under certain assumptions. Let $\mathbf{H}^1_{\mathrm{glob}}$, $\mathbf{H}^1_{\mathrm{loc}}$ be as in §1. We consider the natural map $\mathbf{H}^1_{\mathrm{glob}} \longrightarrow H^1(\mathbf{Q}_n, T) \longrightarrow H^1(\mathbf{Q}_{p,n}, T) \longrightarrow H^1(\mathbf{Q}_{p,n}, T)/(\Phi_n)$, and assume

$(*)_n$ $\qquad \mathbf{H}^1_{\mathrm{glob}} \longrightarrow H^1(\mathbf{Q}_{p,n}, T)/(\Phi_n)$ is not the zero map

for all $n \geq 0$. In particular, condition $(*)_0$ coincides with the condition we considered in §1.4.

Proposition 3.4 *We assume* $(*)_n$ *for all* $n \geq 0$ *and* Problem 0.7. *Then,*
(1) *The cokernel of the natural map* $\mathbf{H}^1_{\mathrm{glob}} \longrightarrow \mathbf{H}^1_{\mathrm{loc}}$ *is pseudo-isomorphic to* Λ.

(2) *If we also assume the Main Conjecture for E (cf. 1.6) and that the p-primary component $Ш(E/\mathbf{Q})[p^\infty]$ of the Tate-Shafarevich group of $E/\mathbf{Q}$ is finite, then* Problem 3.2 *holds.*

Proof. (1) First of all, $\mathbf{H}^1_{\mathrm{glob}}$ is isomorphic to Λ ([9] Theorem 12.4), and as we saw in §1.4, $\mathbf{H}^1_{\mathrm{loc}}$ is isomorphic to $\Lambda \oplus \Lambda$. If we denote by (a, b) the image of a generator of $\mathbf{H}^1_{\mathrm{glob}} \simeq \Lambda$ in $\mathbf{H}^1_{\mathrm{loc}} \simeq \Lambda \oplus \Lambda$, Φ_n does not divide the gcd of a and b. Indeed, if Φ_n divided the gcd of a and b, the map $\mathbf{H}^1_{\mathrm{glob}} \longrightarrow H^1(\mathbf{Q}_{p,n}, T)/(\Phi_n)$ would be a zero map, which contradicts $(*)_n$.

On the other hand, we have an exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathrm{loc}}/\mathbf{H}^1_{\mathrm{glob}} \longrightarrow \mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee_{p^\infty} \longrightarrow \mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee \longrightarrow 0;$$

hence, taking the Λ-torsion parts, we get an exact sequence

$$0 \longrightarrow (\mathbf{H}^1_{\mathrm{loc}}/\mathbf{H}^1_{\mathrm{glob}})_{\Lambda-\mathrm{tors}} \longrightarrow (\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee_{p^\infty})_{\Lambda-\mathrm{tors}} \longrightarrow (\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee)_{\Lambda-\mathrm{tors}}.$$

We write $\mathrm{char}((\mathbf{H}^1_{\mathrm{loc}}/\mathbf{H}^1_{\mathrm{glob}})_{\Lambda-\mathrm{tors}}) = (\epsilon(T))$. By Wingberg [27] Corollary 2.5, we have

$$\mathrm{char}((\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee_{p^\infty})_{\Lambda-\mathrm{tors}}) = \mathrm{char}((\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee)_{\Lambda-\mathrm{tors}}).$$

Hence, by Problem 0.7, any irreducible factor of $\epsilon(T)$ is of the form Φ_n. But Φ_n does not divide the gcd of a and b, so does not divide $\epsilon(T)$. Therefore, $\mathrm{char}((\mathbf{H}^1_{\mathrm{loc}}/\mathbf{H}^1_{\mathrm{glob}})_{\Lambda-\mathrm{tors}}) = (1)$, and $(\mathbf{H}^1_{\mathrm{loc}}/\mathbf{H}^1_{\mathrm{glob}})_{\Lambda-\mathrm{tors}}$ is pseudo-null. This implies $\mathbf{H}^1_{\mathrm{loc}}/\mathbf{H}^1_{\mathrm{glob}} \sim \Lambda$.

(2) Put $h(T) = \Pi_{n\geq 0, e_n \geq 1} \Phi_n^{e_n - 1}$. By the Main Conjecture and Problem 0.7, we have

$$\mathrm{char}(\mathbf{H}^1_{\mathrm{glob}}/ < z_K >) = \mathrm{char}\, \mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee = (h(T)).$$

Hence, we can write $z_K = h(T)\xi$ where ξ is a generator of $\mathbf{H}^1_{\mathrm{glob}}$. By Theorem 1.3, we have $f(T) = \mathrm{Col}^+(\xi)h(T)$ and $g(T) = \mathrm{Col}^-(\xi)h(T)$. We take $a = a(T)$, $b = b(T)$, e_1, e_2 as in the proof of Theorem 0.4 in §1.4, namely, $\xi = ae_1 + be_2$ with a, $b \in \Lambda$. By the proof of Proposition 3.4 (1), a is prime to b. Hence, by Proposition 1.2, the greatest common divisor of $\mathrm{Col}^+(\xi)$ and $\mathrm{Col}^-(\xi)$ is T or 1.

Suppose at first that $e_0 = 0$. Since $Ш(E/\mathbf{Q})[p^\infty]$ is finite, $\mathrm{Sel}(E/\mathbf{Q})_{p^\infty}$ is finite. Hence, by the control theorem for $\mathrm{Sel}^\pm(E/\mathbf{Q}_\infty)$, $\mathrm{char}\, \mathrm{Sel}^\pm(E/\mathbf{Q}_\infty)^\vee \not\subset (T)$. Hence, by the Main Conjecture, $f(0) \neq 0$ and $g(0) \neq 0$. Thus, $\mathrm{Col}^\pm(\xi)(0) \neq 0$. Therefore, the gcd of $\mathrm{Col}^+(\xi)$ and $\mathrm{Col}^-(\xi)$ is 1, and the gcd of $f(T)$ and $g(T)$ is $h(T)$.

Next, suppose $e_0 > 0$. Then, $E(\mathbf{Q}) \otimes \mathbf{Q}_p \longrightarrow E(\mathbf{Q}_p) \otimes \mathbf{Q}_p$ is surjective, so the image of $H^1(\mathbf{Q}, T) \longrightarrow H^1(\mathbf{Q}_p, T)$ is in $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$ by Lemma 1.4. In particular, the image of ξ is in $E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$. Recall that $\xi = a(T)e_1 + b(T)e_2$. Since $\xi \in E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$, we get $a(0) = 0$. It follows from $T \mid \mathrm{Col}^{\pm}(e_2)$ (cf. 1.4) that T divides $\mathrm{Col}^{\pm}(\xi)$. Thus, the gcd of $\mathrm{Col}^{+}(\xi)$ and $\mathrm{Col}^{-}(\xi)$ is T, and the gcd of $f(T)$ and $g(T)$ is $Th(T)$, which completes the proof.

3.3. Examples. Let $E = X_0(17)$ and consider the quadratic twist E_d. The condition of Proposition 3.1 is satisfied for all d such that $0 < d < 250$ except for $d = 104, 193, 233$.

For $d = 104$, we have $r = 2$ and $\lambda(f_d(T)) = \lambda(g_d(T)) = 4$. We know that T^2 divides both $f_d(T)$ and $g_d(T)$, and a computer computation shows that $f_d(T)$ has two addition zeroes of slope 1, and $g_d(T)$ has two addition zeroes of slope $1/2$. Hence, the greatest common divisor of $f_d(T)$ and $g_d(T)$ is T^2 as predicted by Problem 3.2. The computer computations also show that $\mu(f_d(T)) = \mu(g_d(T)) = 0$. Since the Galois representation on the 3-torsion of E_d is surjective, [9] Theorem 13.4 yields that $\mu(\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee) = 0$. Therefore, Proposition 3.3 applies and we have $\mathrm{char}\,\mathrm{Sel}_0(E/\mathbf{Q}_\infty)^\vee = (T)$.

For $d = 233$, we have $r = 1$ and $\min\{\lambda(f_d(T)), \lambda(g_d(T))\} = 3$. In this case, a similar computation can be done and, simply by computing slopes of the zeroes, we can conclude that the gcd of $f_d(T)$ and $g_d(T)$ is T. Again, the relevant μ-invariants are zero and thus Proposition 3.3 yields that $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)$ is finite.

Finally, we consider the case $d = 193$. We have that $\lambda(f_d(T)) = \lambda(g_d(T)) = 7$. However, in this case, both power series have 6 roots of valuation $1/6$ and a simple zero at 0. Thus, simply by looking at slopes of roots, we cannot conclude that their greatest common divisor is T.

To analyze this situation more carefully, we set

$$A(T) = \frac{f_d(T)}{f_d(0)T} \cdot \log^{+}(T) \quad \text{and} \quad B(T) = \frac{g_d(T)}{g_d(0)T} \cdot \frac{\log^{-}(T)}{\Phi_1(T)}$$

which are both convergent power series on the open unit disc. We divide here by $\Phi_1(T)$ so that every root of both $A(T)$ and $B(T)$ has valuation at most $1/6$.

Let π be some 6-th root of p in $\overline{\mathbf{Q}}_p$ and set

$$A'(T) = A(\pi T) \quad \text{and} \quad B'(T) = B(\pi T).$$

Then both A' and B' are convergent power series on the closed unit disc and

are thus in the Tate algebra

$$\mathcal{O}\langle T\rangle = \left\{ f(T) = \sum_{n=0}^{\infty} a_n T^n \ : \ |a_n|_p \to 0 \right\}$$

where $\mathcal{O} = \mathbf{Z}_p[\pi]$.

We consider the image of A' and B' in

$$\mathcal{O}\langle T\rangle/\pi^m \cong (\mathcal{O}/\pi^m\mathcal{O})[T]$$

for various m with the hopes of noticing that the image of these power series do not share a common root in this small polynomial ring.

For $m = 1$, by a computer computation, we have

$$A'(T) \equiv 1 + 2T^6 \ \text{ and } \ B'(T) \equiv 1 + 2T^6,$$

from which we deduce nothing.

For $m = 2$, we have

$$A'(T) \equiv 1 + 2T^6 \ \text{ and } \ B'(T) \equiv 1 + 2\pi T + 2T^6 + \pi T^7.$$

From this, we again deduce nothing as

$$A'(T) \cdot (1 + 2\pi T) \equiv B'(T).$$

For $m = 3$ though, we have

$$A'(T) \equiv 1 + \pi^2 T^2 + 2T^6 \ \text{ and } \ B'(T) \equiv 1 + 2\pi T + \pi^2 T^2 + 2T^6 + \pi T^7 + 2\pi^2 T^8.$$

Now, one computes that

$$B'(T) \equiv A'(T) \cdot (1 + 2\pi T + \pi^2 T^2) + 2\pi^2 T^2.$$

If $\gcd(f_d, g_d) \neq T$, then there exists some common root α in $\mathcal{O}_{\overline{\mathbf{Q}}_p}$ with valuation $1/6$. If we write $\alpha = \pi u$ with u a p-adic unit, then $A'(u) = B'(u) = 0$. But the above identity then forces that $2\pi^2 u^2$ is divisible by π^3, which is impossible! Thus, $\gcd(f_d, g_d) = T$ and $\mathrm{Sel}_0(E/\mathbf{Q}_\infty)$ is finite.

4 Tables

In this section, we present two tables listing the rational points we constructed 3-adically on quadratic twists of $X_0(17)$ and $X_0(32)$. For each curve

$X_0(N)$, we considered d such that $d > 0$, $\gcd(d, 3N) = 1$, and $\operatorname{rank} X_0(N)_d = 1$. In each case, we used the curve's globally minimal Weierstrass equation. For the curve $X_0(17)_d$, we included this equation in the table (by listing the coefficients of $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$). For the curve $X_0(32)_d$, the globally minimal Weierstrass equation is simply $y^2 = x^3 + 4d^2x$.

These computations were done for the curve $X_0(17)$ (resp. $X_0(32)$) using an overconvergent modular symbol that was accurate mod 3^{200} (resp. mod 3^{100}).

Table of global points P_d found on $X_0(17)_d$

d	P_d	$[a_1, a_2, a_3, a_4, a_6]$
5	$(14, -32)$	$[1, -1, 0, -17, -1734]$
28	$\left(\frac{9895}{81}, \frac{-878410}{729}\right)$	$[0, 0, 0, -539, -305270]$
29	$\left(\frac{139064}{1225}, \frac{-46339707}{42875}\right)$	[1,-1,0,-578,-339015]
37	$\left(\frac{150455134}{974169}, \frac{1539419885296}{961504803}\right)$	[1,-1,0,-941,-704158]
40	$(190, -2400)$	$[0, 0, 0, -1100, -890000]$
41	$\left(\frac{1067}{4}, \frac{-34691}{8}\right)$	$[1, -1, 1, -1156, -958144]$
44	$\left(\frac{49351}{441}, \frac{-2413090}{9261}\right)$	$[0, 0, 0, -1331, -1184590]$
56	$\left(\frac{19244}{121}, \frac{-1480800}{1331}\right)$	$[0, 0, 0, -2156, -2442160]$
61	$\left(\frac{3952}{9}, \frac{235937}{27}\right)$	$[1, -1, 0, -2558, -3155815]$
65	$(959, 29095)$	$[1, -1, 1, -2905, -3818278]$
73	$\left(\frac{111991}{36}, \frac{37126789}{216}\right)$	$[1, -1, 1, -3664, -5408852]$
88	$\left(\frac{2140023710080}{8942160969}, \frac{1453764842693104220}{845597567711547}\right)$	$[0, 0, 0, -5324, -9476720]$
92	$\left(\frac{3242226594695}{62457409}, \frac{-5838006309203270250}{493600903327}\right)$	$[0, 0, 0, -5819, -10828630]$
97	$\left(\frac{123907127}{7396}, \frac{1373877614721}{636056}\right)$	$[1, -1, 1, -6469, -12690242]$
109	$\left(\frac{117267845674060}{1957797009}, \frac{-12724817008349896458 55}{86626644257223}\right)$	$[1, -1, 0, -8168, -18006955]$
113	$\left(\frac{23663936531}{729316}, \frac{3630080811299531}{622835864}\right)$	$[1, -1, 1, -8779, -20063092]$
124	$\left(\frac{2195359}{1089}, \frac{-3243299390}{35937}\right)$	$[0, 0, 0, -10571, -26513990]$
133	$\left(\frac{673327635832141}{308624691600}, \frac{-176059882385214150991 09}{171453361171464000}\right)$	$[1, -1, 0, -12161, -32713318]$
173	$\left(\frac{9693514595778788}{18312896333449}, \frac{-653587463274626644218393}{78367421114819312293}\right)$	$[1, -1, 0, -20576, -71997483]$
181	$\left(\frac{56621266}{50625}, \frac{402821517014}{11390625}\right)$	$[1, -1, 0, -22523, -82454830]$
184	$\left(\frac{33961175037484}{73808392329}, \frac{-5571288550874575360}{20052042602765733}\right)$	$[0, 0, 0, -23276, -86629040]$
193	$\left(\frac{915394662845247271}{25061097283236}, \frac{-878088421712236204458830141}{125458509476191439016}\right)$	$[1, -1, 1, -25609, -99966422]$
197	not found	$[1, -1, 0, -26681, -106311798]$
209	$\left(\frac{472269}{400}, \frac{303288257}{8000}\right)$	$[1, -1, 1, -30031, -126947224]$
232	$\left(\frac{1106304238}{1117249}, \frac{-32569057816800}{1180932193}\right)$	$[0, 0, 0, -37004, -173649680]$
233	$\left(\frac{847800975918361973}{716449376631184}, \frac{-738030759904517944421609807}{19176893823953703981248}\right)$	$[1, -1, 1, -37324, -175895512]$
241	$\left(\frac{1313533}{1296}, \frac{-1347623317}{46656}\right)$	$[1, -1, 1, -39931, -194643044]$
248	$\left(\frac{3841589315420}{407192041}, \frac{-7526764618576173000}{8216728195339}\right)$	$[0, 0, 0, -42284, -212111920]$

Table of global points P_d found on $X_0(32)_d$

d	P_d
5	$(5,25)$
13	$(\frac{13}{9}, \frac{845}{27})$
29	$(\frac{1421}{25}, \frac{76531}{125})$
37	$(\frac{37}{441}, \frac{198505}{9261})$
53	$(\frac{750533}{20449}, \frac{1987241095}{2924207})$
61	$(\frac{102541}{1521}, \frac{67889645}{59319})$
77	$(\frac{275625}{719104}, \frac{58139738475}{609800192})$
85	$(765, 21675)$
101	$(\frac{42672500}{9409}, \frac{279031013300}{912673})$
109	$(\frac{5341}{9}, \frac{415835}{27})$
133	$(\frac{314109807025}{1937936484}, \frac{338319926884539145}{85311839898648})$
149	$(\frac{43061}{49}, \frac{9435425}{343})$

References

[1] Bernardi, D. et Perrin-Riou B., Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier), C. R. Acad. Sci. Paris, 317 Sér. I (1993), 227-232.

[2] Coates, J. and Sujatha, R., Fine Selmer groups of elliptic curves over p-adic Lie extensions, Math. Annalen 331 (2005) 809-839.

[3] Colmez, P., Théorie d'Iwasawa des representations de de Rham d'un corps local, Ann. of Math. 148 (1998), 485-571.

[4] Colmez, P., La conjecture de Birch et Swinnerton-Dyer p-adique, Séminaire Bourbaki 919, Astérisque 294 (2004), 251-319.

[5] Cremona, J., `mwrank`, `http://www.maths.nott.ac.uk/personal/jec/ftp/progs/mwrank.info`.

[6] Darmon, H. and Pollack, R., The efficient calculation of Stark-Heegner points via overconvergent modular symbols, Israel Journal of Mathematics 153 (2006), 319-354.

[7] Darmon, H. and Pollack, R., Stark-Heegner point computational package, `http://www.math.mcgill.ca/darmon/programs/shp/shp.html`.

[8] Iwasawa, K., Riemann-Hurwitz formula and p-adic Galois representations for number fields, Tôhoku Math. J. 33 (1981), 263-288.

[9] Kato, K., p-adic Hodge theory and values of zeta functions of modular forms, in *Cohomologies p-adiques et applications arithmétiques III*, Astérisque 295 (2004), 117-290.

[10] Kim, B.-D., The parity theorem of elliptic curves and algebraic functional equations at primes with supersingular reduction, preprint.

[11] Knuth, D. E., *The art of computer programming*, Vol 2., 3rd ed, Addison-Wesley, Reading, Mass. 1997.

[12] Kobayashi, S., Iwasawa theory for elliptic curves at supersingular primes, Invent. math. 152 (2003), 1-36.

[13] Kurihara, M., On the Tate-Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent. math. 149 (2002), 195-224.

[14] The MAGMA computational algebra system, `http://magma.maths.usyd.edu.au`.

[15] Mazur, B. and Tate, J., Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. 54 No 2 (1987), 711-750.

[16] Nekovář, J., On the parity of ranks of Selmer groups II, C. R. Acad. Sci. Paris Sér. I 332 (2001), 99-104.

[17] Perrin-Riou, B., Fonctions L p-adiques d'une courbe elliptique et points rationnels, Ann. Inst. Fourier 43, 4 (1993), 945-995.

[18] Perrin-Riou, B., Théorie d'Iwasawa des representations p-adiques sur un corps local, Invent. math. 115 (1994), 81-149.

[19] Perrin-Riou, B., Arithmétique des courbes elliptiques à reduction supersingulière en p, Experimental Mathematics 12 (2003), 155-186.

[20] Pollack, R., On the p-adic L-functions of a modular form at a supersingular prime, Duke Math. 118 (2003), 523-558.

[21] Pollack, R. and Stevens, G., Explicit computations with overconvergent modular symbols, preprint.

[22] Rubin, K., p-adic variants of the Birch and Swinnerton-Dyer conjecture with complex multiplication, Contemporary Math. 165 (1994), 71-80.

[23] Rubin, K., Euler systems and modular elliptic curves, in *Galois representations in Arithmetic Algebraic Geometry*, London Math. Soc., Lecture Note Series 254 (1998), 351-367.

[24] Skinner, C. and Urban E., Sur les déformations p-adiques des formes de Saito-Kurokawa, C. R. Acad. Sci. Paris, Sér. I 335 (2002), 581-586.

[25] Stein, W., Computing p-adic heights, `http://modular.ucsd.edu/talks/harvard-talk-2004-12-08`.

[26] Stevens, G., Rigid analytic modular symbols, `http://math.bu.edu/people/ghs/research.d`, preprint.

[27] Wingberg, K., Duality theorems for abelian varieties over $\mathbf{Z}_p$-extensions, in *Algebraic Number Theory - in honor of K. Iwasawa*, Advanced Studies in Pure Mathematics 17 (1989), 471-492.

Masato Kurihara
Department of Mathematics,
Keio University,
3-14-1 Hiyoshi, Kohoku-ku,
Yokohama, 223-8522, Japan
`kurihara@math.keio.ac.jp`

Robert Pollack
Department of Mathematics and Statistics
Boston University
Boston, MA 02215, USA
`rpollack@math.bu.edu`